

**United States District Court  
District of Massachusetts (Boston)  
CRIMINAL DOCKET FOR CASE #: 1:11-cr-10260-NMG-1**

Case title: USA v. Swartz

Date Filed: 07/14/2011

Date Terminated: 01/14/2013

---

Assigned to: Judge Nathaniel M. Gorton

**Defendant (1)**

**Aaron Swartz**

*TERMINATED: 01/14/2013*

represented by **Daniel E. Purcell**

Keker & Van Nest, LLP  
633 Battery Street  
San Francisco, CA 94111-1809  
415-391-5400  
Email: [dpurcell@kvn.com](mailto:dpurcell@kvn.com)  
*LEAD ATTORNEY*  
*PRO HAC VICE*  
*ATTORNEY TO BE NOTICED*  
*Designation: Retained*

**Elliot R. Peters**

Keker & Van Nest LLP  
633 Battery Street  
San Francisco, CA 94111  
415-391-5400  
Email: [epeters@kvn.com](mailto:epeters@kvn.com)  
*LEAD ATTORNEY*  
*PRO HAC VICE*  
*ATTORNEY TO BE NOTICED*  
*Designation: Retained*

**Martin G. Weinberg**

Martin G. Weinberg, PC  
20 Park Plaza  
Suite 1000  
Boston, MA 02116  
617-227-3700  
Fax: 617-338-9538  
Email: [owlmcb@att.net](mailto:owlmcb@att.net)  
*TERMINATED: 11/01/2012*  
*LEAD ATTORNEY*  
*ATTORNEY TO BE NOTICED*  
*Designation: Retained*

**Michael J. Pineault**

Clements & Pineault, LLP  
24 Federal Street

Boston, MA 02110  
857-445-0135  
Fax: 857-366-5404  
Email: [mpineault@clementspineault.com](mailto:mpineault@clementspineault.com)  
**LEAD ATTORNEY**  
**ATTORNEY TO BE NOTICED**  
*Designation: Retained*

**Andrew Good**  
Good & Cormier  
3rd Floor  
83 Atlantic Ave.  
Boston, MA 02110  
617-523-5933  
Fax: 617-523-7554  
Email: [agood@goodcormier.com](mailto:agood@goodcormier.com)  
**TERMINATED: 11/03/2011**  
**ATTORNEY TO BE NOTICED**  
*Designation: Retained*

**Matthias A. Kamber**  
Keker & Van Nest LLP  
710 Sansome Street  
San Francisco, CA 94107  
415-391-5400  
Fax: 415-397-7188  
Email: [mkamber@kvn.com](mailto:mkamber@kvn.com)  
**PRO HAC VICE**  
**ATTORNEY TO BE NOTICED**  
*Designation: Retained*

**Pending Counts**

None

**Highest Offense Level (Opening)**

None

**Terminated Counts**

18:1343 & 2... WIRE FRAUD  
(1)  
18:1343 & 2... WIRE FRAUD  
(1s-2s)  
18:1030(a)(4) & 2... COMPUTER FRAUD  
(2)  
18:1030(a)(2), (c)(2)(B)(iii) & 2  
... UNLAWFULLY OBTAINING  
INFORMATION FROM A PROTECTED  
COMPUTER

**Disposition**

**Disposition**

Dismissed on government motion.  
  
Dismissed on government motion.  
  
Dismissed on government motion.  
  
Dismissed on government motion.

(3)

18:1030(a)(4),(b)FRAUD  
(3s-7s)

Dismissed on government motion.

18:1030(a)(5)(B),(c)(4)(A)(i)(I)(VI) &2  
...RECKLESSLY DAMAGING A  
PROTECTED COMPUTER  
(4)

Dismissed on government motion.

18:1030(a)(2),(b),(c)(2)(B)(iii)  
&2...UNLAWFULLY OBTAINING  
INFORMATION FROM A PROTECTED  
COMPUTER  
(8s-12s)

Dismissed on government motion.

18:1030(a)(5),(B),(c)(4)(A)(i)(I),(VI)  
DAMAGING A PROTECTED  
COMPUTER  
(13s)

Dismissed on government motion.

**Highest Offense Level (Terminated)**

Felony

**Complaints**

None

**Disposition**

---

**Plaintiff**

USA

represented by **Scott Garland**  
United States Attorney's Office  
John J. Moakley U.S. Courthouse  
Suite 9200  
Boston, MA 02210  
617-748-3148  
Fax: 617-748-3960  
Email: [scott.garland@usdoj.gov](mailto:scott.garland@usdoj.gov)  
**LEAD ATTORNEY**  
**ATTORNEY TO BE NOTICED**

**Stephen P. Heymann**  
United States Attorney's Office  
John Joseph Moakley Federal Courthouse  
1 Courthouse Way  
Suite 9200  
Boston, MA 02210  
617-748-3100  
Email: [Stephen.Heymann@usdoj.gov](mailto:Stephen.Heymann@usdoj.gov)  
**ATTORNEY TO BE NOTICED**

Date Filed	#	Page	Docket Text
------------	---	------	-------------

07/14/2011	<u>1</u>	16	MOTION to Seal Case as to Aaron Swartz by USA. (Smith3, Dianne) (Entered: 07/14/2011)
07/14/2011		17	Magistrate Judge Timothy S. Hillman: ELECTRONIC ORDER entered granting <u>1</u> Motion to Seal Case as to Aaron Swartz (1) (Smith3, Dianne) (Entered: 07/14/2011)
07/14/2011	<u>2</u>	18	SEALED INDICTMENT as to Aaron Swartz (1) count(s) 1, 2, 3, 4. (Attachments: # <u>1</u> JS45)(Smith3, Dianne) (Entered: 07/14/2011)
07/14/2011	<u>3</u>	36	Arrest Warrant Issued by Magistrate Judge Timothy S. Hillman as to Aaron Swartz. (Smith3, Dianne) (Entered: 07/15/2011)
07/15/2011		35	ELECTRONIC NOTICE of Case Assignment as to Aaron Swartz; Judge Nathaniel M. Gorton assigned to case. If the trial Judge issues an Order of Reference of any matter in this case to a Magistrate Judge, the matter will be transmitted to Chief Magistrate Judge Judith G. Dein. (Rynne, Michelle) (Entered: 07/15/2011)
07/19/2011	<u>4</u>	37	MOTION to Unseal Case as to Aaron Swartz by USA. (Quinn, Thomas) (Entered: 07/19/2011)
07/19/2011		38	Ch. Magistrate Judge Judith G. Dein: ELECTRONIC ORDER entered granting <u>4</u> Motion to Unseal Case as to Aaron Swartz (1) (Quinn, Thomas) (Entered: 07/19/2011)
07/19/2011		39	Attorney update in case as to Aaron Swartz. Attorney Andrew Good added. (Quinn, Thomas) (Entered: 07/19/2011)
07/19/2011		40	Arrest of Aaron Swartz (Quinn, Thomas) (Entered: 07/19/2011)
07/19/2011		41	ELECTRONIC Clerk's Notes for proceedings held before Ch. Magistrate Judge Judith G. Dein:Initial Appearance as to Aaron Swartz held on 7/19/2011, Arraignment as to Aaron Swartz (1) Count 1,2,3,4 held on 7/19/2011, Plea entered by Aaron Swartz (1) Count 1,2,3,4. by Aaron Swartz Not Guilty on counts all. USMJ Dein informs the Dft. of his rights and charges; Dft. has retained counsel; Govt. states maximum penalties; Dft. is released on bond with conditions. 1st conference is set for 9/9/11 @ 10:00am(Attorneys present: Heyman and Good. )Court Reporter Name and Contact or digital recording information: Digital Recording. (Quinn, Thomas) (Entered: 07/19/2011)
07/19/2011	<u>5</u>	42	Appearance and Compliance Bond Entered as to Aaron Swartz in amount of \$ 100,000.00 (Quinn, Thomas) (Entered: 07/19/2011)
07/19/2011	<u>6</u>	43	Ch. Magistrate Judge Judith G. Dein: ORDER entered. ORDER Setting Conditions of Release as to Aaron Swartz. (Quinn, Thomas) (Entered: 07/19/2011)
07/19/2011	<u>7</u>	46	Ch. Magistrate Judge Judith G. Dein: ORDER entered. SCHEDULING ORDER as to Aaron Swartz Status Conference set for 9/9/2011 10:00 AM in Courtroom 15 before Ch. Magistrate Judge Judith G. Dein. (Quinn, Thomas) (Entered: 07/19/2011)
07/19/2011	<u>8</u>	48	Ch. Magistrate Judge Judith G. Dein: ORDER entered. ORDER ON EXCLUDABLE DELAY as to Aaron Swartz. Time excluded from 7/19/11



			until 8/16/11. Reason for entry of order on excludable delay: 18 USC 3161(h)(7)(A) Interests of justice. (Quinn, Thomas) (Entered: 07/19/2011)
07/20/2011	<u>9</u>	50	CORPORATE DISCLOSURE STATEMENT as to Aaron Swartz (Heymann, Stephen) (Entered: 07/20/2011)
07/20/2011	<u>10</u>	52	NOTICE OF ATTORNEY APPEARANCE Scott Garland appearing for USA. (Garland, Scott) (Entered: 07/20/2011)
07/21/2011	<u>11</u>	53	Assented to MOTION Unseal Warrants and Applications, MOTION to Unseal Document ( Responses due by 8/4/2011) as to Aaron Swartz by USA. (Heymann, Stephen) (Entered: 07/21/2011)
07/21/2011	<u>12</u>	55	Motion for Victim Rights in case as to Aaron Swartz( Responses due by 8/4/2011), MOTION For Alternative Victim Notification as to Aaron Swartz by USA. (Heymann, Stephen) (Entered: 07/21/2011)
07/27/2011		58	Ch. Magistrate Judge Judith G. Dein: ELECTRONIC ORDER entered granting <u>11</u> Motion as to Aaron Swartz (1) The US Attorney's Office is responsible to provide copies to the defendant and Middlesex District Attorney's Office. (Quinn, Thomas) (Entered: 08/02/2011)
07/27/2011		59	Ch. Magistrate Judge Judith G. Dein: ELECTRONIC ORDER entered granting <u>12</u> Motion for Victim Rights as to Aaron Swartz (1); granting <u>12</u> Motion as to Aaron Swartz (1) (Quinn, Thomas) (Entered: 08/02/2011)
08/16/2011	<u>13</u>	60	First MOTION for Excludable Delay as to Aaron Swartz by USA. (Attachments: # <u>1</u> Text of Proposed Order)(Heymann, Stephen) (Entered: 08/16/2011)
09/07/2011	<u>14</u>	64	STATUS REPORT ( <i>Joint</i> ) by USA as to Aaron Swartz (Garland, Scott) (Entered: 09/07/2011)
09/08/2011	<u>15</u>	68	MOTION for <i>Leave to Change Residential Address</i> as to Aaron Swartz. (Good, Andrew) (Entered: 09/08/2011)
09/09/2011		70	ELECTRONIC Clerk's Notes for proceedings held before Ch. Magistrate Judge Judith G. Dein: Status Conference as to Aaron Swartz held on 9/9/2011; Counsel report current case status and seek further conference for 11/2/11 @ 2:30pm. Motion hearing is set for 10/11/11 @ 11:00am. (Attorneys present: Garland, Heymann and Good. )Court Reporter Name and Contact or digital recording information: Digital Recording. (Quinn, Thomas) (Entered: 09/12/2011)
09/09/2011	<u>16</u>	71	Ch. Magistrate Judge Judith G. Dein: ORDER entered. STATUS REPORT as to Aaron Swartz Status Conference set for 11/2/2011 02:30 PM in Courtroom 15 before Ch. Magistrate Judge Judith G. Dein. (Quinn, Thomas) (Entered: 09/12/2011)
09/09/2011	<u>17</u>	74	Ch. Magistrate Judge Judith G. Dein: ORDER entered. ORDER ON EXCLUDABLE DELAY as to Aaron Swartz. Time excluded from 8/16/11 until 11/2/11. Reason for entry of order on excludable delay: 18 USC 3161(h)(7)(A) Interests of justice. (Quinn, Thomas) (Entered: 09/12/2011)
09/20/2011		76	Ch. Magistrate Judge Judith G. Dein: ELECTRONIC ORDER entered granting <u>15</u> Motion Change Residential Address as to Aaron Swartz (1)

			(Quinn, Thomas) (Entered: 09/20/2011)
09/27/2011	<u>18</u>	77	MOTION for Protective Order as to Aaron Swartz by USA. (Attachments: # <u>1</u> Text of Proposed Order)(Garland, Scott) (Entered: 09/27/2011)
09/27/2011	<u>19</u>	86	MOTION to Compel <i>Discovery</i> as to Aaron Swartz. (Attachments: # <u>1</u> Exhibit Proposed Order)(Good, Andrew) (Entered: 09/27/2011)
09/27/2011	<u>20</u>	92	MEMORANDUM in Support by Aaron Swartz re <u>19</u> MOTION to Compel <i>Discovery</i> (Attachments: # <u>1</u> Exhibit August 12, 2011 Letter (Good, Andrew) (Additional attachment(s) added on 9/28/2011: (Catino3, Theresa). (Main Document 20 replaced on 9/28/2011...incorrect exhibit attached per request of T. Quinn...) (Catino3, Theresa). (Entered: 09/27/2011)
10/06/2011	<u>21</u>	107	Opposition by Aaron Swartz re <u>18</u> MOTION for Protective Order (Attachments: # <u>1</u> Exhibit JSTOR Announcement)(Good, Andrew) (Entered: 10/06/2011)
10/06/2011	<u>22</u>	119	RESPONSE to Motion by USA as to Aaron Swartz re <u>19</u> MOTION to Compel <i>Discovery</i> (Heymann, Stephen) (Entered: 10/06/2011)
10/06/2011		122	Set/Reset Hearings as to Aaron Swartz Discovery Hearing set for 10/11/2011 11:00 AM in Courtroom 15 before Ch. Magistrate Judge Judith G. Dein. (Quinn, Thomas) (Entered: 10/06/2011)
10/11/2011		123	ELECTRONIC Clerk's Notes for proceedings held before Ch. Magistrate Judge Judith G. Dein: Motion Hearing as to Aaron Swartz held on 10/11/2011 re <u>19</u> MOTION to Compel <i>Discovery</i> filed by Aaron Swartz, <u>18</u> MOTION for Protective Order filed by USA; USMJ Dein hears arguments from Dft., Govt. and victims counsel(Feigelson); supplemental filings are due 10/24/11 and further hearing is set for 11/2/11 @ 2:30pm. (Attorneys present: Garland and Good and Feigelson )Court Reporter Name and Contact or digital recording information: Digital Recording. (Quinn, Thomas) (Entered: 10/13/2011)
10/17/2011		124	Terminate Deadlines and Hearings as to Aaron Swartz: Discovery Hearing. (Moore, Kellyann) (Entered: 10/17/2011)
10/24/2011	<u>23</u>	125	Memorandum regarding Report to the Court re Discovery as to Aaron Swartz (Heymann, Stephen) (Entered: 10/24/2011)
10/24/2011	<u>24</u>	128	MOTION Discovery order re <u>19</u> MOTION to Compel <i>Discovery</i> as to Aaron Swartz. (Attachments: # <u>1</u> Exhibit Proposed Order, # <u>2</u> Exhibit August 12, 2011 Letter)(Good, Andrew) (Entered: 10/24/2011)
10/25/2011	<u>25</u>	149	NOTICE OF ATTORNEY APPEARANCE: Martin G. Weinberg appearing for Aaron Swartz. Type of Appearance: Retained. (Weinberg, Martin) (Entered: 10/25/2011)
10/27/2011	<u>26</u>	150	MOTION to Withdraw as Attorney by Andrew Good as to Aaron Swartz. (Good, Andrew) (Entered: 10/27/2011)
11/02/2011		151	ELECTRONIC Clerk's Notes for proceedings held before Ch. Magistrate Judge Judith G. Dein: Motion Hearing as to Aaron Swartz held on 11/2/2011 re <u>24</u> MOTION Discovery order re <u>19</u> MOTION to Compel <i>Discovery</i> filed by Aaron Swartz, <u>19</u> MOTION to Compel <i>Discovery</i> filed by Aaron Swartz;

			USMJ Dein hears arguments from counsel and victim and continues hearing to 11/8/11 @ 2:30pm. (Attorneys present: Garland and Weinberg. )Court Reporter Name and Contact or digital recording information: Digital Recording. (Quinn, Thomas) (Entered: 11/03/2011)
11/03/2011		152	Ch. Magistrate Judge Judith G. Dein: ELECTRONIC ORDER entered granting <u>26</u> Motion to Withdraw as Attorney Attorney Andrew Good terminated as to Aaron Swartz (1) (Quinn, Thomas) (Entered: 11/03/2011)
11/07/2011		153	Set/Reset Hearings as to Aaron Swartz Discovery Hearing set for 11/8/2011 02:30 PM in Courtroom 15 before Ch. Magistrate Judge Judith G. Dein. (Quinn, Thomas) (Entered: 11/07/2011)
11/08/2011		154	ELECTRONIC Clerk's Notes for proceedings held before Ch. Magistrate Judge Judith G. Dein: Motion Hearing as to Aaron Swartz held on 11/8/2011 re <u>24</u> MOTION Discovery order re <u>19</u> MOTION to Compel <i>Discovery</i> filed by Aaron Swartz, <u>19</u> MOTION to Compel <i>Discovery</i> filed by Aaron Swartz; Counsel report they are working on an agreement on a protective order and the form which discovery will be produced. (Attorneys present: Garland and Weinberg. )Court Reporter Name and Contact or digital recording information: Digital Recording. (Quinn, Thomas) (Entered: 11/09/2011)
11/08/2011	<u>27</u>	155	Ch. Magistrate Judge Judith G. Dein: ORDER entered. ORDER ON EXCLUDABLE DELAY as to Aaron Swartz. Time excluded from 11/2/11 until 12/14/11. Reason for entry of order on excludable delay: 18 USC 3161(h)(7)(A) Interests of justice. (Quinn, Thomas) (Entered: 11/09/2011)
11/30/2011	<u>28</u>	157	Ch. Magistrate Judge Judith G. Dein: ORDER entered. PROTECTIVE ORDER as to Aaron Swartz (Quinn, Thomas) (Entered: 11/30/2011)
12/14/2011		163	ELECTRONIC Clerk's Notes for proceedings held before Ch. Magistrate Judge Judith G. Dein: Status Conference as to Aaron Swartz held on 12/14/2011; Counsel report discovery is ongoing and seek further conference for 1/25/12 @ 10:00am (Attorneys present: Garland and Weinberg. )Court Reporter Name and Contact or digital recording information: Digital Recording – for transcripts or CDs contact Deborah Scalfani by email at deborah_scalfani@mad.uscourts.gov. (Quinn, Thomas) (Entered: 12/14/2011)
12/14/2011	<u>29</u>	164	Ch. Magistrate Judge Judith G. Dein: ORDER entered. STATUS REPORT as to Aaron Swartz Status Conference set for 1/25/2012 10:00 AM in Courtroom 15 before Ch. Magistrate Judge Judith G. Dein. (Quinn, Thomas) (Entered: 12/15/2011)
12/14/2011	<u>30</u>	167	Ch. Magistrate Judge Judith G. Dein: ORDER entered. ORDER ON EXCLUDABLE DELAY as to Aaron Swartz. Time excluded from 12/14/11 until 1/25/12. Reason for entry of order on excludable delay: 18 USC 3161(h)(7)(A) Interests of justice. (Quinn, Thomas) (Entered: 12/15/2011)
01/19/2012	<u>31</u>	169	Joint MOTION for Excludable Delay from January 25, 2012 to March 15, 2012 , Joint MOTION to Reschedule Next Interim Status Conference From January 25, 2012 Until March 15, 2012 ( Responses due by 2/2/2012) as to Aaron Swartz by USA. (Heymann, Stephen) Modified on 1/20/2012 (Jones, Sherry). (Entered: 01/19/2012)

01/20/2012		171	Ch. Magistrate Judge Judith G. Dein: ELECTRONIC ORDER entered granting <u>31</u> Motion to Exclude as to Aaron Swartz (1); granting <u>31</u> Motion to Continue as to Aaron Swartz (1)( Status Conference set for 3/15/2012 02:00 PM in Courtroom 15 before Ch. Magistrate Judge Judith G. Dein.) (Quinn, Thomas) (Entered: 01/20/2012)
01/20/2012	<u>32</u>	172	Ch. Magistrate Judge Judith G. Dein: ORDER entered. ORDER ON EXCLUDABLE DELAY as to Aaron Swartz. Time excluded from 1/25/12 until 3/15/12. Reason for entry of order on excludable delay: 18 USC 3161(h)(7)(A) Interests of justice. (Quinn, Thomas) (Entered: 01/20/2012)
02/01/2012	<u>33</u>	174	Assented to MOTION to Modify Conditions of Release ( <i>Redacted</i> ) as to Aaron Swartz. (Weinberg, Martin) (Entered: 02/01/2012)
02/07/2012		176	Magistrate Judge Judith G. Dein: ELECTRONIC ORDER entered granting <u>33</u> Motion to Modify Conditions of Release as to Aaron Swartz (1) (Quinn, Thomas) (Entered: 02/07/2012)
03/08/2012	<u>34</u>	177	STATUS REPORT <i>Filed Jointly by the Parties</i> by USA as to Aaron Swartz (Heymann, Stephen) (Entered: 03/08/2012)
03/16/2012	<u>35</u>	180	Magistrate Judge Judith G. Dein: ORDER entered. STATUS REPORT as to Aaron Swartz Status Conference set for 5/17/2012 02:30 PM in Courtroom 15 before Magistrate Judge Judith G. Dein. (Quinn, Thomas) (Entered: 03/19/2012)
03/16/2012	<u>36</u>	182	Magistrate Judge Judith G. Dein: ORDER entered. ORDER ON EXCLUDABLE DELAY as to Aaron Swartz. Time excluded from 3/1/12 until 5/17/12. Reason for entry of order on excludable delay: 18 USC 3161(h)(7)(A) Interests of justice. (Quinn, Thomas) (Main Document 36 replaced on 5/22/2012) (Quinn, Thomas). (Entered: 03/19/2012)
03/19/2012		184	Set/Reset Hearings as to Aaron Swartz Status Conference set for 5/17/2012 02:30 PM in Courtroom 15 before Magistrate Judge Judith G. Dein. (Quinn, Thomas) (Entered: 03/19/2012)
04/27/2012		185	ELECTRONIC NOTICE OF RESCHEDULING from 5/17/12 to 5/22/12 from as to Aaron Swartz Status Conference set for 5/22/2012 02:30 PM in Courtroom 15 before Magistrate Judge Judith G. Dein. (Quinn, Thomas) (Entered: 04/27/2012)
05/16/2012	<u>37</u>	186	JOINT STATUS REPORT by Aaron Swartz (Weinberg, Martin) Modified docket text on 5/16/2012 (Moore, Kellyann). (Entered: 05/16/2012)
05/22/2012		189	ELECTRONIC Clerk's Notes for proceedings held before Magistrate Judge Judith G. Dein: Status Conference as to Aaron Swartz held on 5/22/2012; Counsel report discovery is ongoing and seek further conference for 7/26/12 @ 2:30pm.(Attorneys present: Heymann and Weinberg. )Court Reporter Name and Contact or digital recording information: Digital Recording – for transcripts or CDs contact Deborah Scalfani (deborah_scalfani@mad.uscourts.gov). (Quinn, Thomas) (Entered: 05/22/2012)
05/23/2012	<u>38</u>	190	Magistrate Judge Judith G. Dein: ORDER entered. STATUS REPORT as to Aaron Swartz Status Conference set for 7/26/2012 02:30 PM in Courtroom 15 before Magistrate Judge Judith G. Dein. (Quinn, Thomas) (Entered: 05/23/2012)

			05/23/2012)
05/23/2012	<u>39</u>	192	Magistrate Judge Judith G. Dein: ORDER entered. ORDER ON EXCLUDABLE DELAY as to Aaron Swartz. Time excluded from 5/17/12 until 7/26/12. Reason for entry of order on excludable delay: 18 USC 3161(h)(7)(A) Interests of justice. (Quinn, Thomas) (Entered: 05/23/2012)
06/01/2012	<u>40</u>	194	MOTION for Discovery as to Aaron Swartz. (Attachments: # <u>1</u> Exhibit A, # <u>2</u> Exhibit B, # <u>3</u> Exhibit C)(Weinberg, Martin) (Entered: 06/01/2012)
06/22/2012	<u>41</u>	207	RESPONSE to Motion by USA as to Aaron Swartz re <u>40</u> MOTION for Discovery (Heymann, Stephen) (Entered: 06/22/2012)
07/25/2012	<u>42</u>	218	STATUS REPORT by Aaron Swartz (Weinberg, Martin) (Entered: 07/25/2012)
07/26/2012	<u>43</u>	221	ELECTRONIC Clerk's Notes for proceedings held before Magistrate Judge Judith G. Dein: Final Status Conference as to Aaron Swartz held on 7/26/2012, Motion Hearing as to Aaron Swartz held on 7/26/2012 re <u>40</u> MOTION for Discovery filed by Aaron Swartz; Counsel report current case status; USMJ Dein hears arguments on motion and takes motion under advisement. Court Reporter Name and Contact or digital recording information: Digital Recording – for transcripts or CDs contact Deborah Scalfani (deborah_scalfani@mad.uscourts.gov). (Quinn, Thomas) (Entered: 07/27/2012)
08/01/2012	<u>44</u>	222	Magistrate Judge Judith G. Dein: ORDER entered. REPORT AND ORDER on Final Status Conference as to Aaron Swartz Discovery to be completed by 8/15/2012; dispositive motion are due 9/28/12 and Govt. response to dispositive motions due 10/30/12. (Quinn, Thomas) (Entered: 08/01/2012)
08/01/2012	<u>45</u>	224	Magistrate Judge Judith G. Dein: ORDER entered. ORDER ON EXCLUDABLE DELAY as to Aaron Swartz. Time excluded from 7/26/12 until 10/30/12. Reason for entry of order on excludable delay: 18 USC 3161(h)(7)(A) Interests of justice. (Quinn, Thomas) (Entered: 08/01/2012)
08/01/2012	<u>46</u>	226	Magistrate Judge Judith G. Dein: ORDER entered granting in part and denying in part <u>40</u> Motion for Discovery as to Aaron Swartz (1) (Quinn, Thomas) (Entered: 08/01/2012)
08/01/2012	<u>47</u>	231	Magistrate Judge Judith G. Dein: ELECTRONIC ORDER entered finding as moot <u>18</u> Motion for Protective Order as to Aaron Swartz (1); finding as moot <u>19</u> Motion to Compel as to Aaron Swartz (1); finding as moot <u>24</u> Motion as to Aaron Swartz (1); finding as moot <u>11</u> Motion to Unseal Document as to Aaron Swartz (1); finding as moot <u>13</u> Motion to Exclude as to Aaron Swartz (1) (Quinn, Thomas) (Entered: 08/01/2012)
08/01/2012		232	Judge update in case as to Aaron Swartz. Magistrate Judge Judith G. Dein no longer assigned to case. (Quinn, Thomas) (Entered: 08/01/2012)
08/02/2012	<u>48</u>	233	Judge Nathaniel M. Gorton: ELECTRONIC ORDER entered acknowledging <u>44</u> Report and Order on Final Status Conference by Magistrate Judge as to Aaron Swartz (1) Interim Pretrial Conference set for 8/15/2012 02:30 PM in Courtroom 4 before Judge Nathaniel M. Gorton. (Patch, Christine) (Entered: 08/02/2012)



08/15/2012	49	234	ELECTRONIC Clerk's Notes for proceedings held before Judge Nathaniel M. Gorton: Interin Pretrial Conference as to Aaron Swartz held on 8/15/2012. Counsel anticipate trial lasting 2 weeks. Jury Trial set for 2/4/2013 09:00 AM in Courtroom 4 before Judge Nathaniel M. Gorton. Government's initial expert disclosures by 11/19/12, Defendant's by 12/10/12, and additional experts by 12/31/12. Motions in limine due by 1/14/2013; oppositions to Motions in Limine, Exhibit/Witness Lists, and proposed voir dire due by 1/21/2013; objections to exhibit/witness lists, proposed jury instructions, and proposed verdict form due by 1/21/2013. Government to file assented-to Motion to Exclude all time between 8/15/12 and 2/4/13. (Attorneys present: Weinberg, Heymann. )Court Reporter Name and Contact or digital recording information: Cheryl Dahlstrom (617-951-4555). (Patch, Christine) (Entered: 08/15/2012)
08/15/2012		235	Terminate Deadlines and Hearings as to Aaron Swartz: Interim Pretrial Conference held on 8/15/12. (Patch, Christine) (Entered: 08/15/2012)
08/17/2012	<u>50</u>	236	Assented to MOTION for Speedy Trial <i>Exclusion</i> as to Aaron Swartz by USA. (Heymann, Stephen) (Entered: 08/17/2012)
08/24/2012	51	238	Judge Nathaniel M. Gorton: ELECTRONIC ORDER entered granting <u>50</u> Motion for Speedy Trial as to Aaron Swartz (1) (Patch, Christine) (Entered: 08/24/2012)
08/24/2012	<u>52</u>	239	Judge Nathaniel M. Gorton: ORDER entered. ORDER ON EXCLUDABLE DELAY as to Aaron Swartz. Time excluded from August 15, 2012 until February 4, 2013. Reason for entry of order on excludable delay: 18 USC 3161(h)(7)(A) Interests of justice. (Patch, Christine) (Entered: 08/24/2012)
09/12/2012	<u>53</u>	240	SUPERSEDING INDICTMENT as to Aaron Swartz (1) count(s) 1s-2s, 3s-7s, 8s-12s, 13s. (Attachments: # <u>1</u> JS45)(Smith3, Dianne) (Entered: 09/12/2012)
09/12/2012	54	258	Judge Nathaniel M. Gorton: ELECTRONIC ORDER entered. Order Referring Case to Magistrate Judge Judith G. Dein Reason for referral: P as to Aaron Swartz (Smith3, Dianne) (Entered: 09/12/2012)
09/14/2012	<u>55</u>	259	Assented to MOTION for Extension of Time to File as to Aaron Swartz. (Weinberg, Martin) (Entered: 09/14/2012)
09/20/2012	56	261	ELECTRONIC NOTICE OF HEARING as to Aaron Swartz Arraignment set for 9/24/2012 11:00 AM in Courtroom 15 before Magistrate Judge Judith G. Dein. (Quinn, Thomas) (Entered: 09/20/2012)
09/24/2012	57	262	ELECTRONIC Clerk's Notes for proceedings held before Magistrate Judge Judith G. Dein:Arraignment as to Aaron Swartz (1) Count 1s-2s,3s-7s,8s-12s,13s held on 9/24/2012, Plea entered by Aaron Swartz Not Guilty on counts all. (Attorneys present: Garland and Weinberg. )Court Reporter Name and Contact or digital recording information: Digital Recording – for transcripts or CDs contact Deborah Scalfani (deborah_scalfani@mad.uscourts.gov). (Quinn, Thomas) (Entered: 09/25/2012)
09/24/2012	58	263	Magistrate Judge Judith G. Dein: ELECTRONIC ORDER entered granting <u>55</u> Motion for Extension of Time as to Aaron Swartz (1) (Quinn, Thomas)

			(Entered: 09/25/2012)
09/25/2012		264	Judge update in case as to Aaron Swartz. Magistrate Judge Judith G. Dein no longer assigned to case. (Quinn, Thomas) (Entered: 09/25/2012)
10/05/2012	<u>59</u>	265	MOTION to Suppress as to Aaron Swartz. (Weinberg, Martin) (Entered: 10/05/2012)
10/05/2012	<u>60</u>	286	MOTION to Suppress as to Aaron Swartz. (Weinberg, Martin) (Entered: 10/05/2012)
10/05/2012	<u>61</u>	307	MOTION to Suppress as to Aaron Swartz. (Weinberg, Martin) (Entered: 10/05/2012)
10/05/2012	<u>62</u>	319	MOTION to Suppress as to Aaron Swartz. (Weinberg, Martin) (Entered: 10/05/2012)
10/05/2012	<u>63</u>	330	MOTION to Suppress as to Aaron Swartz. (Weinberg, Martin) (Entered: 10/05/2012)
10/05/2012	<u>64</u>	336	MOTION to Dismiss as to Aaron Swartz. (Weinberg, Martin) (Entered: 10/05/2012)
10/05/2012	65	347	ELECTRONIC NOTICE issued requesting courtesy copy for <u>63</u> MOTION to Suppress, <u>61</u> MOTION to Suppress, <u>62</u> MOTION to Suppress, <u>64</u> MOTION to Dismiss, <u>59</u> MOTION to Suppress, <u>60</u> MOTION to Suppress as to Aaron Swartz Counsel who filed these documents are requested to submit a courtesy copy of them to the Clerk's Office. <b>These documents must be clearly marked as a Courtesy Copy and reflect the document number assigned by CM/ECF.</b> (Patch, Christine) (Entered: 10/05/2012)
10/10/2012	67	348	Judge Nathaniel M. Gorton: ELECTRONIC ORDER entered granting 66 Motion to Seal as to Aaron Swartz (1) (Patch, Christine) (Entered: 10/10/2012)
10/10/2012	<u>68</u>	349	Sealed EXHIBITS by Aaron Swartz <u>63</u> MOTION to Suppress filed by Aaron Swartz, <u>61</u> MOTION to Suppress filed by Aaron Swartz, 65 Notice requesting courtesy copy,, <u>62</u> MOTION to Suppress filed by Aaron Swartz, <u>64</u> MOTION to Dismiss filed by Aaron Swartz, <u>59</u> MOTION to Suppress filed by Aaron Swartz, <u>60</u> MOTION to Suppress filed by Aaron Swartz (Patch, Christine) (Entered: 10/10/2012)
10/31/2012	<u>69</u>	350	NOTICE OF ATTORNEY APPEARANCE: Matthias A. Kamber appearing for Aaron Swartz. Type of Appearance: Retained. (Kamber, Matthias) (Entered: 10/31/2012)
10/31/2012	<u>70</u>	352	MOTION to Withdraw as Attorney by Martin Weinberg as to Aaron Swartz. (Weinberg, Martin) (Entered: 10/31/2012)
11/01/2012	71	354	Judge Nathaniel M. Gorton: ELECTRONIC ORDER entered granting <u>70</u> Motion to Withdraw as Attorney Attorney Martin G. Weinberg terminated as to Aaron Swartz (1) (Patch, Christine) (Entered: 11/01/2012)
11/08/2012	<u>72</u>	355	Assented to MOTION Extension of Response Brief Deadline, Permission to File Response Brief Exceeding Local Rule's Page Limits, and Filing a Reply Brief re <u>63</u> MOTION to Suppress, <u>61</u> MOTION to Suppress, <u>62</u> MOTION to Suppress, <u>64</u> MOTION to Dismiss, <u>59</u> MOTION to Suppress, <u>60</u>

			MOTION to Suppress as to Aaron Swartz by USA. (Garland, Scott) (Entered: 11/08/2012)
11/08/2012	<u>73</u>	357	NOTICE OF ATTORNEY APPEARANCE: Michael J. Pineault appearing for Aaron Swartz. Type of Appearance: Retained. (Pineault, Michael) (Entered: 11/08/2012)
11/08/2012	<u>74</u>	359	Assented to MOTION for Leave to Appear Pro Hac Vice by Elliot R. Peters Filing fee \$ 100, receipt number 0101-4195066. as to Aaron Swartz. (Attachments: # <u>1</u> Exhibit A, # <u>2</u> Proposed Order)(Pineault, Michael) (Entered: 11/08/2012)
11/08/2012	<u>75</u>	366	Assented to MOTION for Leave to Appear Pro Hac Vice by Daniel E. Purcell Filing fee \$ 100, receipt number 0101-4195073. as to Aaron Swartz. (Attachments: # <u>1</u> Exhibit A, # <u>2</u> Proposed Order)(Pineault, Michael) (Entered: 11/08/2012)
11/09/2012	76	373	Judge Nathaniel M. Gorton: ELECTRONIC ORDER entered granting <u>74</u> Motion for Leave to Appear Pro Hac Vice Added Elliot R. Peters. <b>Attorneys admitted Pro Hac Vice must register for electronic filing if the attorney does not already have an ECF account in this district. To register go to the Court website at www.mad.uscourts.gov. Select Case Information, then Electronic Filing (CM/ECF) and go to the CM/ECF Registration Form.</b> as to Aaron Swartz (1); granting <u>75</u> Motion for Leave to Appear Pro Hac Vice Added Daniel E. Purcell. <b>Attorneys admitted Pro Hac Vice must register for electronic filing if the attorney does not already have an ECF account in this district. To register go to the Court website at www.mad.uscourts.gov. Select Case Information, then Electronic Filing (CM/ECF) and go to the CM/ECF Registration Form.</b> as to Aaron Swartz (1) (Moore, Kellyann) (Entered: 11/09/2012)
11/13/2012	77	375	Judge Nathaniel M. Gorton: ELECTRONIC ORDER entered granting in part and denying in part <u>72</u> Assented to MOTION Extension of Response Brief Deadline, Permission to File Response Brief Exceeding Local Rule's Page Limits, and Filing a Reply Brief as to Aaron Swartz by USA. "The Government may file a consolidated brief in opposition to defendant's motions to suppress and it may do so by November 16. Defendant is granted leave to file a reply brief by December 3. The Government's consolidated brief, however, may not exceed 55 pages and the Defendant's reply is not to exceed 10 pages." (Moore, Kellyann) (Entered: 11/13/2012)
11/16/2012	<u>81</u>	376	RESPONSE to Motion by USA as to Aaron Swartz re <u>63</u> MOTION to Suppress, <u>61</u> MOTION to Suppress, <u>59</u> MOTION to Suppress, <u>62</u> MOTION to Suppress, <u>60</u> MOTION to Suppress (Attachments: # <u>1</u> Exhibit JSTOR Policy Before Download, # <u>2</u> Exhibit JSTOR Policy Cover Sheet, # <u>3</u> Exhibit JSTOR's Terms of Service, # <u>4</u> Exhibit MIT's Guest Rules of Use, # <u>5</u> Exhibit Guerilla Open Access Manifesto, # <u>6</u> Exhibit MIT Guest Registration, # <u>7</u> Exhibit MIT Registration and DHCP Log Excerpts, # <u>8</u> Exhibit Building 16 Door and No Trespassing Sign, # <u>9</u> Exhibit Wiring Closet Exterior, # <u>10</u> Exhibit Wiring Closet Interior and Cardboard Box, # <u>11</u> Exhibit Equipment in Closet, # <u>12</u> Exhibit Network Cable and Network Switch, # <u>13</u> Exhibit January 4 Entrance, # <u>14</u> Exhibit January 6 Entrance, # <u>15</u> Exhibit January 6 Packing, # <u>16</u> Exhibit January 6 Exit, # <u>17</u> Exhibit Equipment in Building 20, # <u>18</u> Exhibit MIT Records Policy, # <u>19</u> Exhibit



			Arrest Report, # <u>20</u> Exhibit BELegislative History, # <u>21</u> Exhibit USB Drive Search Warrant, # <u>22</u> Exhibit MIT Policy)(Garland, Scott) (Entered: 11/16/2012)
11/16/2012	<u>82</u>	518	RESPONSE to Motion by USA as to Aaron Swartz re <u>64</u> MOTION to Dismiss <i>Counts 1 and 2</i> (Heymann, Stephen) (Entered: 11/16/2012)
11/30/2012	<u>85</u>	532	Assented to MOTION for Hearing <i>Status Conference</i> as to Aaron Swartz by USA. (Heymann, Stephen) (Entered: 11/30/2012)
12/03/2012	<u>86</u>	534	MOTION for Leave to File <i>REPLY BRIEFING AND EXHIBIT UNDER SEAL</i> as to Aaron Swartz. (Peters, Elliot) (Entered: 12/03/2012)
12/03/2012	<u>87</u>	537	REPLY TO RESPONSE to Motion by Aaron Swartz re <u>63</u> MOTION to Suppress , <u>61</u> MOTION to Suppress , <u>62</u> MOTION to Suppress , <u>64</u> MOTION to Dismiss , <u>59</u> MOTION to Suppress , <u>60</u> MOTION to Suppress <i>DEFENDANT'S REPLY IN SUPPORT OF MOTIONS TO SUPPRESS AND MOTION TO DISMISS COUNTS 1 AND 2 OF SUPERSEDING INDICTMENT [REDACTED VERSION]</i> (Peters, Elliot) (Entered: 12/03/2012)
12/03/2012	<u>88</u>	548	MOTION to Continue <i>DEFENDANT'S MOTION FOR CONTINUANCE OF TRIAL DATE AND EXPERT DISCLOSURE DEADLINE</i> to June 10, 2013 to Continue trial date as to Aaron Swartz. (Peters, Elliot) (Entered: 12/03/2012)
12/03/2012	<u>89</u>	551	MEMORANDUM in Support by Aaron Swartz re <u>88</u> MOTION to Continue <i>DEFENDANT'S MOTION FOR CONTINUANCE OF TRIAL DATE AND EXPERT DISCLOSURE DEADLINE</i> to June 10, 2013 to Continue trial date (Peters, Elliot) (Entered: 12/03/2012)
12/03/2012	<u>90</u>	556	RESPONSE to Motion by Aaron Swartz re <u>85</u> Assented to MOTION for Hearing <i>Status Conference DEFENDANT'S RESPONSE TO GOVERNMENT'S MOTION FOR A STATUS CONFERENCE</i> (Peters, Elliot) (Entered: 12/03/2012)
12/03/2012	91	559	Judge Nathaniel M. Gorton: ELECTRONIC ORDER entered granting <u>85</u> Motion for Hearing as to Aaron Swartz (1) (Patch, Christine) (Entered: 12/03/2012)
12/03/2012	92	560	ELECTRONIC NOTICE OF HEARING as to Aaron Swartz Status Conference set for 12/14/2012 02:00 PM in Courtroom 4 before Judge Nathaniel M. Gorton. (Patch, Christine) (Entered: 12/03/2012)
12/04/2012	93	561	Judge Nathaniel M. Gorton: ELECTRONIC ORDER entered granting <u>86</u> Motion for Leave to File Reply Briefing and Exhibit Under Seal. (Patch, Christine) (Entered: 12/04/2012)
12/04/2012	<u>94</u>	562	SEALED REPLY in Support of <u>63</u> MOTION to Suppress , <u>61</u> MOTION to Suppress , <u>62</u> MOTION to Suppress , <u>64</u> MOTION to Dismiss , <u>59</u> MOTION to Suppress , <u>60</u> MOTION to Suppress by Aaron Swartz. (Attachments: # <u>1</u> Exhibit 1, # <u>2</u> Cover Letter)(Moore, Kellyann) (Entered: 12/04/2012)
12/05/2012	<u>95</u>	563	RESPONSE to Motion by USA as to Aaron Swartz re <u>88</u> MOTION to Continue <i>DEFENDANT'S MOTION FOR CONTINUANCE OF TRIAL DATE AND EXPERT DISCLOSURE DEADLINE</i> to June 10, 2013 to

			Continue trial date (Heymann, Stephen) (Entered: 12/05/2012)
12/14/2012	96	565	ELECTRONIC Clerk's Notes for proceedings held before Judge Nathaniel M. Gorton: Interim Status Conference as to Aaron Swartz held on 12/14/2012 (Attorneys present: Hayman, Peters, Pineault, Purcell (by phone). )Court Reporter Name and Contact or digital recording information: Cheryl Dahlstrom (617-951-4555). Court is in session. Court hears from the parties as to the necessity of an evidentiary hearing. Court orders hearing on 1/25/2013 at 1:00 p.m. Experts designated by 1/25/2013. Trial to begin on 4/1/2013. (Hohler, Daniel) (Entered: 12/14/2012)
12/14/2012	97	566	ELECTRONIC NOTICE OF HEARING as to Aaron Swartz Evidentiary Hearing set for 1/25/2013 01:00 PM in Courtroom 4 before Judge Nathaniel M. Gorton. Jury Trial set for 4/1/2013 09:00 AM in Courtroom 4 before Judge Nathaniel M. Gorton. (Hohler, Daniel) (Entered: 12/14/2012)
12/17/2012	<u>98</u>	567	Judge Nathaniel M. Gorton: ORDER entered. NOTICE. Please see order for details. (Moore, Kellyann) (Entered: 12/18/2012)
12/18/2012	99	569	Set/Reset Deadlines/Hearings as to Aaron Swartz: Expert Witness List due by 1/25/2013. Evidentiary Hearing set for 1/25/2013 01:30 PM in Courtroom 4 before Judge Nathaniel M. Gorton. (Moore, Kellyann) (Entered: 12/18/2012)
01/07/2013	<u>100</u>	570	MOTION for Leave to File <i>DEFENDANT AARON SWARTZ'S MOTION FOR LEAVE TO FILE SUPPLEMENTAL MEMORANDUM IN SUPPORT OF MOTIONS TO SUPPRESS</i> as to Aaron Swartz. (Attachments: # <u>1</u> Exhibit 1)(Peters, Elliot) (Entered: 01/07/2013)
01/10/2013	<u>101</u>	581	Assented to MOTION for Leave to File <i>Response to Defendant's Supplemental Memorandum in Support of His Motion to Dismiss</i> as to Aaron Swartz by USA. (Attachments: # <u>1</u> Government's Response, # <u>2</u> Exhibit A to Government's Response, # <u>3</u> Exhibit B to Government's Response)(Heymann, Stephen) (Entered: 01/10/2013)
01/11/2013	102	588	Judge Nathaniel M. Gorton: ELECTRONIC ORDER entered granting <u>100</u> Motion for Leave to File as to Aaron Swartz (1); granting <u>101</u> Motion for Leave to File as to Aaron Swartz (1); Counsel using the Electronic Case Filing System should now file the document for which leave to file has been granted in accordance with the CM/ECF Administrative Procedures. Counsel must include – Leave to file granted on (date of order)– in the caption of the document (Patch, Christine) (Entered: 01/11/2013)
01/11/2013	<u>103</u>	589	Supplemental MEMORANDUM in Support by Aaron Swartz re <u>63</u> MOTION to Suppress <i>DEFENDANT AARON SWARTZ'S SUPPLEMENTAL MEMORANDUM IN SUPPORT OF MOTIONS TO SUPPRESS</i> (Attachments: # <u>1</u> Exhibit A)(Peters, Elliot) (Entered: 01/11/2013)
01/11/2013	<u>104</u>	596	Supplemental MEMORANDUM in Opposition by USA as to Aaron Swartz re <u>63</u> MOTION to Suppress <i>No. 5</i> (Attachments: # <u>1</u> Exhibit Evidence Transfer Chronology, # <u>2</u> Exhibit Finger Print Report Excerpt)(Heymann, Stephen) (Entered: 01/11/2013)
01/14/2013	<u>105</u>	602	DISMISSAL as to Aaron Swartz (Heymann, Stephen) (Entered: 01/14/2013)
01/14/2013	<u>106</u>	603	

		Judge Nathaniel M. Gorton: ORDER entered. DISMISSAL OF COUNTS on Government Motion as to Aaron Swartz. Counts dismissed: All counts dismissed. (Patch, Christine) (Entered: 01/14/2013)
--	--	---

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA )

v. )

Aaron Swartz )

Criminal No. 11-CR-10260

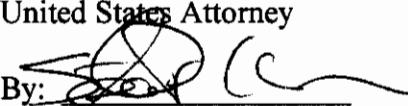
**GOVERNMENT'S MOTION TO SEAL  
INDICTMENT**

7/14/11, Sealed  
Pursuant to FRCP 6(e)(4), the United States of America hereby moves this Court to direct that the indictment be sealed (and that no person shall disclose the return of the indictment except when necessary for the issuance and execution of a warrant) until the defendant is in custody in the above-captioned case and the Court has ordered the indictment unsealed.

The United States further moves pursuant to General Order 06-05 that the United States Attorney, through undersigned counsel, be provided copies of all sealed documents which the United States has filed in this matter.

Respectfully submitted,

CARMEN M. ORTIZ  
United States Attorney

By:   
Stephen P. Heymann  
Assistant U.S. Attorney

Date: July 14, 2011

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:3959362@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260 \*SEALED\* USA v. Swartz Order on Motion to Seal Case  
Content-Type: text/html

***NOTE: This docket entry (or case) is sealed, no email notices have been sent.***

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 7/14/2011 at 3:13 PM EDT and filed on 7/14/2011

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260 \*SEALED\*

**Filer:**

**Document Number:** No document attached

**Docket Text:**

**Magistrate Judge Timothy S. Hillman: ELECTRONIC ORDER entered granting [1] Motion to Seal Case as to Aaron Swartz (1) (Smith3, Dianne)**

**1:11-cr-10260 \*SEALED\*-1 No electronic public notice will be sent because the case/entry is sealed.**

**UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS**

**UNITED STATES OF AMERICA**

**v.**

**AARON SWARTZ,**

**Defendant**

**Crim. No.**

*11-cr-10260*

**VIOLATIONS:**

**18 U.S.C. § 1343 (Wire Fraud)**

**18 U.S.C. § 1030(a)(4) (Computer Fraud)**

**18 U.S.C. § 1030(a)(2), (c)(2)(B)(iii)  
(Unlawfully Obtaining Information from a  
Protected Computer)**

**18 U.S.C. § 1030(a)(5)(B), (c)(4)(A)(i)(I),(VI)  
(Recklessly Damaging a Protected Computer)**

**18 U.S.C. § 2 (Aiding and Abetting)**

**18 U.S.C. § 981(a)(1)(C), 28 U.S.C. § 2461(c),  
and 18 U.S.C. § 982(a)(2)(B) (Criminal  
Forfeiture)**

**INDICTMENT**

The Grand Jury charges that at all relevant times:

***PARTIES***

1. The Massachusetts Institute of Technology ("MIT") was and continued to be a leading research and teaching university located in Cambridge, Massachusetts.

2. JSTOR, founded in 1995, was and continued to be a United States-based, not-for-profit organization that provides an online system for archiving and providing access to academic journals. It provides searchable digitized copies of over 1,000 academic journals, dating back for lengthy periods of time.

3. JSTOR's service is important to research institutions and universities because it can be extraordinarily expensive, in terms of both cost and space, for a research or university library to maintain a comprehensive collection of academic journals. By digitizing extensive, historical collections of journals, JSTOR enables libraries to outsource the journals' storage,

ensures their preservation, and enables authorized users to conduct full-text, cross-disciplinary searches of them. JSTOR has invested millions of dollars in obtaining and digitizing the journal articles that it makes available as part of its service.

4. JSTOR generally charges libraries, universities, and publishers a subscription fee for access to JSTOR's digitized journals. For a large research university, this annual subscription fee for JSTOR's various collections of content can cost more than \$50,000. Portions of the subscription fees are shared with the journal publishers who hold the original copyrights. In addition, JSTOR makes some articles available for individual purchase. Publishers decide which articles can be purchased individually and set fees for their articles. JSTOR facilitates the purchase of these articles from the archive on behalf of the participating publishers.

5. JSTOR did not permit users:

- a. to download or export content from its computer servers with automated computer programs such as web robots, spiders and scrapers;
- b. to download all of the articles from any particular issue of a journal; or
- c. to make other than personal use of individually downloaded articles.

6. JSTOR notified its users of these rules, and users accepted these rules when they chose to obtain and use JSTOR's content.

7. JSTOR provided MIT with its services and content for a fee.

8. MIT, in turn, made JSTOR's services and content available to its students, faculty, and employees. MIT also allowed guests of the Institute to have the same access as its students, faculty, and employees for short periods of time while they were on campus.

9. JSTOR's computers were located outside the Commonwealth of Massachusetts, and thus any communications between JSTOR's computers and MIT's computers in Massachusetts crossed state boundaries. JSTOR's computers were also used in and affected interstate and foreign commerce.

10. Aaron Swartz lived in the District of Massachusetts and was a fellow at Harvard



University's Center for Ethics. Although Harvard provided Swartz access to JSTOR's services and archive as needed for his research, Swartz used MIT's computer networks to steal well over 4,000,000 articles from JSTOR. Swartz was not affiliated with MIT as a student, faculty member, or employee or in any other manner other than his and MIT's common location in Cambridge. Nor was Swartz affiliated in any way with JSTOR.

### ***OVERVIEW OF THE OFFENSES***

11. Between September 24, 2010, and January 6, 2011, Swartz contrived to:
  - a. break into a restricted computer wiring closet at MIT;
  - b. access MIT's network without authorization from a switch within that closet;
  - c. connect to JSTOR's archive of digitized journal articles through MIT's computer network;
  - d. use this access to download a major portion of JSTOR's archive onto his computers and computer hard drives;
  - e. avoid MIT's and JSTOR's efforts to prevent this massive copying, measures which were directed at users generally and at Swartz's illicit conduct specifically; and
  - f. elude detection and identification;

all with the purpose of distributing a significant proportion of JSTOR's archive through one or more file-sharing sites.

### ***MEANS OF COMMITTING THE OFFENSES***

12. Swartz alone, or in knowing concert with others unknown to the grand jury, (hereafter simply "Swartz" in this section) committed these offenses through the means described below.

*September 24 through 27, 2010*

13. On September 24, 2010, Swartz purchased an Acer laptop computer from a local



computer store with the intent of using it to automatically and systematically harvest JSTOR's archive of digitized journal articles.

14. Later that day, Swartz connected the Acer computer to MIT's computer network from a location in Building 16 at MIT and registered under a pseudonym with MIT's computer network as a guest. MIT offers campus guests short-term service on its computer network. Campus guests must register on the MIT network and are limited to a total of fourteen days per year of network service.

15. Swartz registered on the network using identifiers chosen to hide his identity as the computer's owner and user.

a. The computer was registered under the fictitious guest name "Gary Host."

b. The computer's client name was specified as "ghost laptop." A computer's client name helps to identify it on a network and can be chosen by its user. In this case, the name was simply created by abridging the pseudonym "Gary Host," combining the first initial "g" with the last name "host."

c. The fictitious "Gary Host's" e-mail address was identified as "ghost@mailinator.com." This was a "throwaway" e-mail address. Mailinator is a free, disposable e-mail service that allows a user to create a new e-mail address as needed, without even registering the address with Mailinator. Mailinator provides this service for users to have an anonymous and temporary e-mail address. Mailinator accepts mail for any e-mail address directed to the mailinator.com domain without need for a prior registration, and it allows anyone in the world to read that mail without having to create an account or enter a password. All mail sent to mailinator.com is automatically deleted after several hours whether read or not.

16. On September 25, 2010, Swartz used the Acer laptop to systematically access and rapidly download an extraordinary volume of articles from JSTOR. He used a software program

to automate the downloading process so that a human being would not need to keep typing in the archive requests. The program was also designed to sidestep or confuse JSTOR's efforts to prevent this behavior.

17. These rapid and massive downloads and download requests impaired computers used by JSTOR to service client research institutions and threatened to misappropriate its archive.

18. As JSTOR, and then MIT, became aware of these efforts to steal a vast proportion of JSTOR's archive, each took steps to block the flow of articles to Swartz's computer and thus to prevent him from redistributing them. Swartz, in turn, repeatedly altered the appearance of his Acer laptop and the apparent source of his automated demands to get around JSTOR's and MIT's blocks against his computer.

a. On the evening of September 25, 2010, JSTOR blocked the computer's access to its network by refusing communications from the computer's assigned IP address. An IP (short for "Internet Protocol") address is a unique numeric address used by a computer on the Internet. Every computer attached to the Internet must be assigned an IP address so the Internet traffic sent from and directed to that computer can be directed properly from the source to its destination. Most Internet service providers control a range of IP Addresses. MIT controls all IP addresses that begin with the number 18. In this case, the computer had been assigned an IP address of 18.55.6.215, and JSTOR blocked communications from that IP address.

b. On September 26, 2010, Swartz obtained for his computer a new IP address on the MIT network – 18.55.6.216 – and began again to download an extraordinary volume of articles from JSTOR. Accesses from this address continued until the middle of the day, when JSTOR spotted and blocked this IP address as well. Because the exploits on September 25 and 26 were both

launched from MIT IP addresses beginning with 18.55.6 , and because computers used by JSTOR to service client research institutions were again impaired and its archive at risk of misappropriation, on September 26, 2010, JSTOR began blocking a much broader range of IP addresses. As a result, legitimate JSTOR users at MIT were denied access to JSTOR's archive until September 29, 2010.

c. Notified by JSTOR of what was happening, MIT sought to block Swartz more specifically. It did so by prohibiting the Acer laptop from being assigned an IP address on MIT's network. When a user plugs his computer into the wired network on MIT's campus, his computer's MAC address is used to determine whether he has been authorized to use the network. A MAC address is a unique identifier assigned to a computer network interface, in this case, the Acer laptop's network interface card. A MAC address most often is assigned by the manufacturer of the network interface card and therefore generally remains constant on the device. Although a MAC address is intended to be a permanent and globally unique identification, a user with the right knowledge can change the MAC address, an action referred to as "MAC address spoofing," as discussed below.

d. As part of the registration process, "Gary Host's" computer, i.e., the Acer laptop, had identified its network interface's MAC address as 00:23:5a:73:5f:fb. Consequently, on September 27, 2010, MIT deactivated the guest registration for the "ghost laptop" by barring any network interface with that MAC address from being assigned a new IP address.

19. MIT banned the Acer laptop from its network under and consistent with its own computer use rules, which required users to:

a. use the network to support MIT's research, education, and MIT administrative activities, or at least to not interfere with these activities;

- b. maintain the system's security and conform to applicable laws, including copyright laws; and
- c. conform with rules imposed by any networks to which users connected through MIT's system.

Guest users of the MIT network agreed to be bound by the same rules that applied to students, faculty, and employees. These rules explicitly notified users that violations could lead to state or federal prosecution.

*October 2 through 9, 2010*

20. Despite knowing that his computer had been blocked from JSTOR's and MIT's networks, Swartz sought and obtained another guest connection on MIT's network, again for his Acer laptop less than a week later, on October 2, 2010.

21. Once again, Swartz registered the Acer laptop on the network using identifiers chosen to avoid identifying Swartz as the computer's owner and user:

- a. The computer was once again registered under the fictitious name "Gary Host" and the client name "ghost laptop."
- b. To evade the MAC address block, Swartz spoofed the computer's MAC address, manipulating it from 00:23:5a:73:5f:fb to 00:23:5a:73:5f:fc (the final "b" became a "c").
- c. By re-registering the "ghost laptop," Swartz ensured that it was assigned a new IP address. By obtaining a new IP address, Swartz disassociated his rogue computer from the IP addresses used to exploit JSTOR in September.

22. On October 8, 2010, Swartz connected a second computer to MIT's network and registered as a guest, using similar naming conventions: the computer was registered under the name "Grace Host," the computer client name "ghost macbook," and the throw-away e-mail address "ghost42@mailinator.com."

23. The next day, October 9, 2010, Swartz used both the "ghost laptop" and the

“ghost macbook” to systematically and rapidly access and download an extraordinary volume of articles from JSTOR. The pace was so fast that it brought down some of JSTOR’s computer servers.

24. In response, JSTOR blocked the entire MIT computer network’s access to JSTOR for several days, beginning on or about October 9, 2010.

*November and December, 2010*

25. During November and December, 2010, Swartz used the “ghost laptop” (i.e., the Acer laptop) at MIT to make over two million downloads from JSTOR. This is more than one hundred times the number of downloads during the same period by all the legitimate MIT JSTOR users combined. Of the downloads, approximately half were research articles, with the remainder being reviews, news, editorials, and miscellaneous documents.

26. This time around, Swartz circumvented MIT’s guest registration process altogether when he connected to MIT’s computer network. By this point, Swartz was familiar with the IP addresses available to be assigned at the switch in the restricted network interface closet in the basement of MIT’s Building 16. Swartz simply hard-wired into the network and assigned himself two IP addresses. He hid the Acer laptop and a succession of external storage drives under a box in the closet, so that they would not be obvious to anyone who might enter the closet.

*January 4 through 6, 2011*

27. On January 4, 2011, Aaron Swartz was observed entering the restricted basement network wiring closet to replace an external hard drive attached to his computer.

28. On January 6, 2011, Swartz returned to the wiring closet to remove his computer equipment. This time he attempted to evade identification at the entrance to the restricted area. As Swartz entered the wiring closet, he held his bicycle helmet like a mask to shield his face, looking through ventilation holes in the helmet. Swartz then removed his computer equipment from the closet, put it in his backpack, and left, again masking his face with the bicycle helmet



before peering through a crack in the double doors and cautiously stepping out.

29. Shortly thereafter, Swartz connected the Acer laptop to MIT's network in a different building, again registering on the network using identifiers chosen to avoid identifying Swartz as the computer's owner and user.

a. The computer was registered under the fictitious name "Grace Host" and the client name "ghost laptop."

b. To evade the block on the computer's MAC address, Swartz had spoofed (manipulated) its MAC address a second time, changing it from the blocked 00:23:5a:73:5f:fb to 00:4c:e5:a0:c7:56.

c. By re-registering the "ghost laptop," Swartz ensured that it was assigned a new IP address. By obtaining a new IP address for his rogue computer, Swartz disassociated it from the IP addresses used to exploit JSTOR up to that point.

30. Swartz had a software program named "keepgrabbing.py" installed on the Acer laptop. Keepgrabbing.py was designed to download .pdf files from jstor.org and sidestep or confuse JSTOR's efforts to prevent the behavior.

31. When MIT Police spotted Swartz on the afternoon of January 6, 2011 and attempted to question him, he fled with a USB drive that contained the program "keepgrabbing2.py." "Keepgrabbing2.py" had distinct similarities to "keepgrabbing.py."

32. In all, Swartz stole approximately 4.8 million articles, a major portion of the total archive in which JSTOR had invested. Of these, approximately 1.7 million were made available by independent publishers for purchase through JSTOR's Publisher Sales Service.

33. Swartz intended to distribute a significant portion of JSTOR's archive of digitized journal articles through one or more file-sharing sites.

**COUNT 1**  
**Wire Fraud**  
**18 U.S.C. §§ 1343 & 2**

34. The Grand Jury realleges and incorporates by reference the allegations in paragraphs 1-33 of this Indictment and charges that:

From on or about September 24, 2010, through January 6, 2011, or thereabout, in the District of Massachusetts and elsewhere, the defendant,

**AARON SWARTZ,**

having devised and intended to devise a scheme and artifice to defraud and for obtaining property — namely, journal articles digitized and distributed by JSTOR, and copies thereof — by means of material false and fraudulent pretenses, representations, and promises, transmitted and caused to be transmitted by means of wire communication in interstate commerce writings, signs, signals, and pictures — namely, communications to and from JSTOR’s computer servers — for the purpose of executing the scheme, and aided and abetted the same.

All in violation of Title 18, United States Code, Sections 1343 and 2.

**COUNT 2**  
**Computer Fraud**  
**18 U.S.C. §§ 1030(a)(4) & 2**

35. The Grand Jury realleges and incorporates by reference the allegations in paragraphs 1-33 of this Indictment and charges that:

From on or about September 24, 2010, through January 6, 2011, or thereabout, in the District of Massachusetts and elsewhere, the defendant,

**AARON SWARTZ,**

knowingly and with intent to defraud, accessed a protected computer — namely, a computer on MIT's network and a computer on JSTOR's network — without authorization and in excess of authorized access, and by means of such conduct furthered the intended fraud and obtained things of value — namely, digitized journal articles from JSTOR's archive — and aided and abetted the same.

All in violation of Title 18, United States Code, Sections 1030(a)(4) and 2.



**COUNT 3**  
**Unlawfully Obtaining Information from a Protected Computer**  
**18 U.S.C. §§ 1030(a)(2), (c)(2)(B)(iii) & 2**

36. The Grand Jury realleges and incorporates by reference the allegations in paragraphs 1-33 of this Indictment and charges that:

From on or about September 24, 2010, through January 6, 2011, or thereabout, in the District of Massachusetts and elsewhere, the defendant,

**AARON SWARTZ,**

intentionally accessed a computer — namely, a computer on MIT’s computer network and a computer on JSTOR’s network — without authorization and in excess of authorized access, and thereby obtained from a protected computer information whose value exceeded \$5,000 — namely, digitized journal articles from JSTOR’s archive — and aided and abetted the same.

All in violation of 18 U.S.C. §§ 1030(a)(2), (c)(2)(B)(iii) and 2.

**COUNT 4**  
**Recklessly Damaging a Protected Computer**  
**18 U.S.C. §§ 1030(a)(5)(B), (c)(4)(A)(i)(I),(VI) & 2**

37. The Grand Jury realleges and incorporates by reference the allegations in paragraphs 1-33 of this Indictment and charges that:

From on or about September 24, 2010, through January 6, 2011, or thereabout, in the District of Massachusetts and elsewhere, the defendant,

**AARON SWARTZ,**

intentionally accessed a protected computer — namely, a computer on MIT's computer network and a computer on JSTOR's network — without authorization, and as a result of such conduct recklessly caused damage to MIT and JSTOR, and, during a 1-year period, caused loss aggregating at least \$5,000 in value and damage affecting at least 10 protected computers, and aided and abetted the same.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(B), (c)(4)(A)(i)(I),(VI) & 2.

**FORFEITURE ALLEGATIONS**

**(18 U.S.C. § 981(a)(1)(C), 28 U.S.C. § 2461(c), and 18 U.S.C. §982(a)(2)(B))**

38. Upon conviction of the offense alleged in Count One of the Indictment, the defendant,

**AARON SWARTZ,**

shall forfeit to the United States, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), any property, real or personal, that constitutes, or is derived from, proceeds traceable to the commission of the offense.

39. Upon conviction of one or more of the offenses alleged in Counts Two through Four of the Indictment, the defendant,

**AARON SWARTZ,**

shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(2)(B) any property constituting, or derived from, proceeds obtained directly or indirectly as a result of the commission of the offenses.

40. If any of the property described in paragraphs 38 and 39 hereof as being forfeitable pursuant to 18 U.S.C. § 981(a)(1)(C), 28 U.S.C. § 2461(c), and 18 U.S.C. § 982(a)(2)(B) as a result of any act or omission of the defendant --

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred to, sold to, or deposited with a third party;
- c. has been placed beyond the jurisdiction of this Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

it is the intention of the United States, pursuant to 21 U.S.C. § 853(p), as incorporated by 28 U.S.C. § 2461(c), to seek forfeiture of all other property of the defendant up to the value of the property described in paragraphs 38 and 39 above.

All pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(2)(B), and Title 28, United States Code, Section 2461(c).

A TRUE BILL

David R Thompson  
Foreperson of the Grand Jury

[Signature]  
Assistant United States Attorney

Date: 7-14-11

DISTRICT OF MASSACHUSETTS

July 14, 2011

Returned into the District Court by the Grand Jurors and filed.

[Signature]  
Deputy Clerk  
2:00p

JS 45 (5/97) - (Revised U.S.D.C. MA 3/25/2011)

**Criminal Case Cover Sheet****U.S. District Court - District of Massachusetts**Place of Offense: \_\_\_\_\_ Category No. II Investigating Agency Secret ServiceCity Cambridge**Related Case Information:**County Middlesex

Superseding Ind./ Inf. \_\_\_\_\_ Case No. \_\_\_\_\_

Same Defendant \_\_\_\_\_ New Defendant \_\_\_\_\_

Magistrate Judge Case Number \_\_\_\_\_

Search Warrant Case Number \_\_\_\_\_ See Additional Information Below

R 20/R 40 from District of \_\_\_\_\_

**Defendant Information:**Defendant Name Aaron Swartz Juvenile: ☐ Yes ☒ NoIs this person an attorney and/or a member of any state/federal bar: ☐ Yes ☒ No


Alias Name \_\_\_\_\_

Address (City & State) Cambridge, MA Birth date (Yr only): 86 SSN (last4#): 1374 Sex M Race: W Nationality: USADefense Counsel if known: Andrew Good Address Good & CourmierBar Number \_\_\_\_\_ 83 Atlantic Ave.U.S. Attorney Information: \_\_\_\_\_ Boston, MA 02110AUSA Stephen Heymann Bar Number if applicable 558486Interpreter: ☐ Yes ☒ No List language and/or dialect: \_\_\_\_\_Victims: ☒ Yes ☐ No If yes, are there multiple crime victims under 18 USC§3771(d)(2) ☒ Yes ☐ NoMatter to be SEALED: ☒ Yes ☐ No☒ Warrant Requested ☐ Regular Process ☐ In Custody**Location Status:**

Arrest Date \_\_\_\_\_

☐ Already in Federal Custody as of \_\_\_\_\_ in \_\_\_\_\_☐ Already in State Custody at \_\_\_\_\_ ☐ Serving Sentence ☐ Awaiting Trial☐ On Pretrial Release: Ordered by: \_\_\_\_\_ on \_\_\_\_\_Charging Document: ☐ Complaint ☐ Information ☒ IndictmentTotal # of Counts: ☐ Petty \_\_\_\_\_ ☐ Misdemeanor \_\_\_\_\_ ☒ Felony 4

Continue on Page 2 for Entry of U.S.C. Citations

☒ I hereby certify that the case numbers of any prior proceedings before a Magistrate Judge are accurately set forth above.Date: July 14, 2011 Signature of AUSA: 

JS 45 (5/97) (Revised U.S.D.C. MA 12/7/05) Page 2 of 2 or Reverse

District Court Case Number (To be filled in by deputy clerk): \_\_\_\_\_

Name of Defendant Aaron Swartz

## U.S.C. Citations

	<u>Index Key/Code</u>	<u>Description of Offense Charged</u>	<u>Count Numbers</u>
Set 1	<u>18 USC 1343</u>	<u>Wire Fraud</u>	<u>1</u>
Set 2	<u>18 USC 1030(a)(4)</u>	<u>Computer Fraud</u>	<u>2</u>
Set 3	<u>18 USC 1030(a)(2)</u>	<u>Theft of Information From a Computer</u>	<u>3</u>
Set 4	<u>18 USC 1030(a)(5)(B)</u>	<u>Recklessly Damaging a Computer</u>	<u>4</u>
Set 5	<u>18 USC 981 &amp; 982 and 28 USC 2461</u>	<u>Forfeiture</u>	
Set 6	<u>18 USC 2</u>	<u>Aiding and Abetting</u>	<u>Counts 1-4</u>
Set 7	_____	_____	_____
Set 8	_____	_____	_____
Set 9	_____	_____	_____
Set 10	_____	_____	_____
Set 11	_____	_____	_____
Set 12	_____	_____	_____
Set 13	_____	_____	_____
Set 14	_____	_____	_____
Set 15	_____	_____	_____

**ADDITIONAL INFORMATION:** Search Warrant Case Numbers: 11m-5013-JGD; 11m-5014-JGD  
11m-5015-JGD; 11m-5031-JGD; 11m-5061-JGD; 11m-5062-JGD; 11m-5063-JGD; and  
11m-5143-JGD

**Seizure Warrant Case Number:** 11m-5138-JGD

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:3961083@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG \*SEALED\* USA v. Swartz Case Assigned/Reassigned  
Content-Type: text/html

***NOTE: This docket entry (or case) is sealed, no email notices have been sent.***

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 7/15/2011 at 1:02 PM EDT and filed on 7/15/2011

**Case Name:** USA v. Swartz  
**Case Number:** 1:11-cr-10260-NMG \*SEALED\*  
**Filer:**  
**Document Number:** No document attached

**Docket Text:**

**ELECTRONIC NOTICE of Case Assignment as to Aaron Swartz; Judge Nathaniel M. Gorton assigned to case. If the trial Judge issues an Order of Reference of any matter in this case to a Magistrate Judge, the matter will be transmitted to Chief Magistrate Judge Judith G. Dein. (Rynne, Michelle)**

**1:11-cr-10260-NMG \*SEALED\*-1 No electronic public notice will be sent because the case/entry is sealed.**

## UNITED STATES DISTRICT COURT

for the

District of Massachusetts

United States of America

v.

Aaron Swartz

Defendant

Case No. 11-cr-10260

## ARREST WARRANT

To: Any authorized law enforcement officer

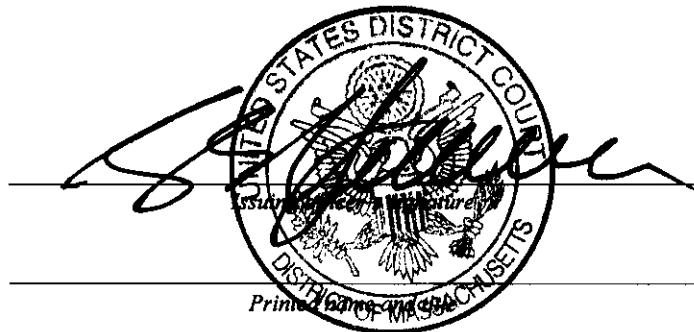
**YOU ARE COMMANDED** to arrest and bring before a United States magistrate judge without unnecessary delay(name of person to be arrested) Aaron Swartz,

who is accused of an offense or violation based on the following document filed with the court:

- ☒ Indictment   
 ☐ Superseding Indictment   
 ☐ Information   
 ☐ Superseding Information   
 ☐ Complaint  
☐ Probation Violation Petition   
☐ Supervised Release Violation Petition   
☐ Violation Notice   
☐ Order of the Court

This offense is briefly described as follows:

18 U.S.C. 1343 (Wire Fraud); 18 U.S.C. 1030(a)(4) (Computer Fraud); 18 U.S.C. 1030 (a)(2) (Theft of Information From a Computer) and 18 U.S.C. 1030 (a)(5)(B) (Recklessly Damaging a Computer); 18 U.S.C. 2 (Aiding and Abetting)  
 All committed between September 24, 2010 and January 6, 2011, or thereabout

Date: July 14, 2011City and state: Boston, Massachusetts

## Return

This warrant was received on (date) \_\_\_\_\_, and the person was arrested on (date) \_\_\_\_\_  
 at (city and state) \_\_\_\_\_.

Date: \_\_\_\_\_

Arresting officer's signature

Printed name and title



UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA )

v. )

AARON SWARTZ )

Criminal No. 11-CR-10260-NMG

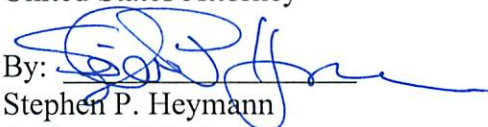
**GOVERNMENT'S MOTION TO UNSEAL  
INDICTMENT**

The United States of America hereby moves this Court to direct that the indictment be unsealed. In support of this motion, the government states that the defendant surrendered himself this morning, and that there is no further reason to keep the indictment secret.

Dein, M.J.  
MOTION ALLOWED  
By the Court  
Deputy Clerk  
7/19/2011

Respectfully submitted,

CARMEN M. ORTIZ  
United States Attorney

By:   
Stephen P. Heymann  
Assistant U.S. Attorney

Date: July 19, 2011

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:3964673@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz \*SEALED\* Order on Motion to Unseal Case  
Content-Type: text/html

***NOTE: This docket entry (or case) is sealed, no email notices have been sent.***

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 7/19/2011 at 9:40 AM EDT and filed on 7/19/2011

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG \*SEALED\*

**Filer:**

**Document Number:** No document attached

**Docket Text:** \*Sealed Entry\*

**Ch. Magistrate Judge Judith G. Dein: ELECTRONIC ORDER entered granting [4] Motion to Unseal Case as to Aaron Swartz (1) (Quinn, Thomas)**

**1:11-cr-10260-NMG \*SEALED\*-1 No electronic public notice will be sent because the case/entry is sealed.**

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:3966502@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Add and Terminate Attorneys  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 7/19/2011 at 5:18 PM EDT and filed on 7/19/2011

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** No document attached

**Docket Text:**

**Attorney update in case as to Aaron Swartz. Attorney Andrew Good added. (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Stephen P. Heymann Stephen.Heymann@usdoj.gov, janet.smith@usdoj.gov, usama.ecf@usdoj.gov

Andrew Good agood@goodcormier.com, hill@goodcormier.com, josh@goodcormier.com,  
lpetrova@goodcormier.com, pcormier@goodcormier.com

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:3966504@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Arrest  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 7/19/2011 at 5:19 PM EDT and filed on 7/19/2011

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** No document attached

**Docket Text:**

**Arrest of Aaron Swartz (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Stephen P. Heymann Stephen.Heymann@usdoj.gov, janet.smith@usdoj.gov, usama.ecf@usdoj.gov

Andrew Good agood@goodcormier.com, hill@goodcormier.com, josh@goodcormier.com,  
lpetrova@goodcormier.com, pcormier@goodcormier.com

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:3966509@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Terminate Deadlines  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 7/19/2011 at 5:23 PM EDT and filed on 7/19/2011

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** No document attached

**Docket Text:**

**ELECTRONIC Clerk's Notes for proceedings held before Ch. Magistrate Judge Judith G. Dein:Initial Appearance as to Aaron Swartz held on 7/19/2011, Arraignment as to Aaron Swartz (1) Count 1,2,3,4 held on 7/19/2011, Plea entered by Aaron Swartz (1) Count 1,2,3,4. by Aaron Swartz Not Guilty on counts all. USMJ Dein informs the Dft. of his rights and charges; Dft. has retained counsel; Govt. states maximum penalties; Dft. is released on bond with conditions. 1st conference is set for 9/9/11 @ 10:00am(Attorneys present: Heyman and Good. )Court Reporter Name and Contact or digital recording information: Digital Recording. (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Stephen P. Heymann Stephen.Heymann@usdoj.gov, janet.smith@usdoj.gov, usama.ecf@usdoj.gov

Andrew Good agood@goodcormier.com, hill@goodcormier.com, josh@goodcormier.com,  
lpetrova@goodcormier.com, pcormier@goodcormier.com

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

UNITED STATES DISTRICT COURT

District of

Massachusetts

UNITED STATES OF AMERICA

V.

APPEARANCE AND COMPLIANCE BOND

Aaron Swartz  
Defendant

Case Number:

11-10260

Non-surety: I, the undersigned defendant acknowledge that I and my . . .

Surety: We, the undersigned, jointly and severally acknowledge that we and our . . .

personal representatives, jointly and severally, are bound to pay to the United States of America the sum of

\$ 100,000.00

, and there has been deposited in the Registry of the Court the sum of

\$ 0

in cash or (describe other security.)

The conditions of this bond are that the defendant,

Aaron Swartz  
(Name)

is to (1) appear before this court and at such other places as the defendant may be required to appear, in accordance with any and all orders and directions relating to the defendant's appearance in this case, including appearance for violation of a condition of defendant's release as may be ordered or notified by this court or any other United States District Court to which the defendant may be held to answer or the cause transferred; (2) comply with all conditions of release imposed by the court, and (3) abide by any judgment entered in such matter by surrendering to serve any sentence imposed and obeying any order or direction in connection with such judgment.

It is agreed and understood that this is a continuing bond (including any proceeding on appeal or review) which shall continue until such time as the undersigned are exonerated.

If the defendant appears as ordered or notified and otherwise obeys and performs the foregoing conditions of this bond, then this bond is to be void, but if the defendant fails to obey or perform any of these conditions, payment of the amount of this bond shall be due forthwith. Forfeiture of this bond for any breach of its conditions may be declared by any United States District Court having cognizance of the above entitled matter at the time of such breach and if the bond is forfeited and if the forfeiture is not set aside or remitted, judgment, may be entered upon motion in such United States District Court against each debtor jointly and severally for the amount above stated, together with interest and costs, and execution may be issued and payment secured as provided by the Federal Rules of Criminal Procedure and any other laws of the United States.

This bond is signed on

7/19/2011  
Date

at

U.S.D.C. Boston MA  
Place

Defendant

Aaron Swartz

Address

Cambridge, MA

Surety

Swartz

Address

Highland Park, IL

Surety

Swartz

Address

Highland Park, IL

Signed and acknowledged before me

7/19/2011  
Date

Thomas L. Gandy  
Judge/Clerk

Approved

Judge Officer



UNITED STATES DISTRICT COURT  
for the

United States of America

v.

Case No. 11-10260Sean Swartz  
Defendant

**ORDER SETTING CONDITIONS OF RELEASE**

IT IS ORDERED that the defendant's release is subject to these conditions:

- ✓ (1) The defendant must not violate any federal, state or local law while on release.
- ✓ (2) The defendant must cooperate in the collection of a DNA sample if the collection is authorized by 42 U.S.C. § 14135a.
- ✓ (3) The defendant must immediately advise the court, defense counsel, and the U.S. attorney in writing before any change in address or telephone number.
- ✓ (4) The defendant must appear in court as required and must surrender to serve any sentence imposed

The defendant must appear at (if blank, to be notified) \_\_\_\_\_

Place

on \_\_\_\_\_

Date and Time

**Release on Personal Recognizance or Unsecured Bond**

IT IS FURTHER ORDERED that the defendant be released on condition that:

( ✓ ) (5) The defendant promises to appear in court as required and surrender to serve any sentence imposed.

( ✓ ) (6) The defendant executes an unsecured bond binding the defendant to pay to the United States the sum of One hundred thousand and 00/100 dollars (\$ 100,000.00) in the event of a failure to appear as required or surrender to serve any sentence imposed.



## ADDITIONAL CONDITIONS OF RELEASE

Upon finding that release by one of the above methods will not by itself reasonably assure the defendant's appearance and the safety of other persons or the community, IT IS FURTHER ORDERED that the defendant's release is subject to the conditions marked below:

( ) (7) The defendant is placed in the custody of:

Person or organization \_\_\_\_\_

Address (only if above is an organization) \_\_\_\_\_

City and state \_\_\_\_\_

Tel. No. (only if above is an organization) \_\_\_\_\_

who agrees (a) to supervise the defendant in accordance with all of the conditions of release, (b) to use every effort to assure the defendant's appearance at all scheduled court proceedings, and (c) to notify the court immediately if the defendant violates any condition of release or disappears.

Signed: \_\_\_\_\_

Custodian or Proxy

Date

( ) (8) The defendant must:

( ) (a) report to the Pretrial Services as directed  
telephone number \_\_\_\_\_, no later than \_\_\_\_\_

( ) (b) execute a bond or an agreement to forfeit upon failing to appear as required the following sum of money or designated property:

( ) (c) post with the court the following proof of ownership of the designated property, or the following amount or percentage of the above-described sum

( ) (d) execute a bail bond with solvent sureties in the amount of \$ \_\_\_\_\_

( ) (e) maintain or actively seek employment.

( ) (f) maintain or commence an education program.

( ) (g) surrender any passport to: \_\_\_\_\_

( ) (h) obtain no passport.

( ) (i) abide by the following restrictions on personal association, place of abode, or travel: maintain current residence

have a restricted to admitted United States

( ) (j) avoid all contact, directly or indirectly, with any person who is or may become a victim or potential witness in the investigation or prosecution, including but not limited to: \_\_\_\_\_

( ) (k) undergo medical or psychiatric treatment: as directed

( ) (l) return to custody each (week) day at \_\_\_\_\_ o'clock after being released each (week) day at \_\_\_\_\_ o'clock for employment, schooling, or the following purpose(s): \_\_\_\_\_

( ) (m) maintain residence at a halfway house or community corrections center, as the pretrial services office or supervising officer considers necessary.

( ) (n) refrain from possessing a firearm, destructive device, or other dangerous weapons.

( ) (o) refrain from ( ) any ( ) excessive use of alcohol.

( ) (p) refrain from use or unlawful possession of a narcotic drug or other controlled substances defined in 21 U.S.C. § 802, unless prescribed by a licensed medical practitioner.

( ) (q) submit to any testing required by the pretrial services office or the supervising officer to determine whether the defendant is using a prohibited substance. Any testing may be used with random frequency and include urine testing, the wearing of a sweat patch, a remote alcohol testing system, and/or any form of prohibited substance screening or testing. The defendant must refrain from obstructing or attempting to obstruct or tamper, in any fashion, with the efficiency and accuracy of any prohibited substance testing or monitoring which is (are) required as a condition of release.

( ) (r) participate in a program of inpatient or outpatient substance abuse therapy and counseling if the pretrial services office or supervising officer considers it advisable.

( ) (s) participate in one of the following location monitoring program components and abide by its requirements as the pretrial services officer or supervising officer instructs.

( ) (i) **Curfew.** You are restricted to your residence every day ( ) from \_\_\_\_\_ to \_\_\_\_\_, or ( ) as directed by the pretrial services office or supervising officer; or

( ) (ii) **Home Detention.** You are restricted to your residence at all times except for employment; education; religious services; medical, substance abuse, or mental health treatment; attorney visits; court appearances; court-ordered obligations; or other activities pre-approved by the pretrial services office or supervising officer; or

( ) (iii) **Home Incarceration.** You are restricted to 24-hour-a-day lock-down except for medical necessities and court appearances or other activities specifically approved by the court.

( ) (t) submit to the location monitoring indicated below and abide by all of the program requirements and instructions provided by the pretrial services officer or supervising officer related to the proper operation of the technology.

( ) The defendant must pay all or part of the cost of the program based upon your ability to pay as the pretrial services office or supervising officer determines.

( ) (i) Location monitoring technology as directed by the pretrial services office or supervising officer;

( ) (ii) Radio Frequency (RF) monitoring;

( ) (iii) Passive Global Positioning Satellite (GPS) monitoring;

( ) (iv) Active Global Positioning Satellite (GPS) monitoring (including "hybrid" (Active/Passive) GPS);

( ) (v) Voice Recognition monitoring.

( ) (u) stay away from M.I.T. campus

DISTRIBUTION: COURT DEFENDANT PRETRIAL SERVICES U.S. ATTORNEY U.S. MARSHAL



**ADVICE OF PENALTIES AND SANCTIONS**

TO THE DEFENDANT:

YOU ARE ADVISED OF THE FOLLOWING PENALTIES AND SANCTIONS:

Violating any of the foregoing conditions of release may result in the immediate issuance of a warrant for your arrest, a revocation of your release, an order of detention, a forfeiture of any bond, and a prosecution for contempt of court and could result in imprisonment, a fine, or both.

While on release, if you commit a federal felony offense the punishment is an additional prison term of not more than ten years and for a federal misdemeanor offense the punishment is an additional prison term of not more than one year. This sentence will be consecutive (*i.e.*, in addition to) to any other sentence you receive.

It is a crime punishable by up to ten years in prison, and a \$250,000 fine, or both, to: obstruct a criminal investigation; tamper with a witness, victim, or informant; retaliate or attempt to retaliate against a witness, victim, or informant; or intimidate or attempt to intimidate a witness, victim, juror, informant, or officer of the court. The penalties for tampering, retaliation, or intimidation are significantly more serious if they involve a killing or attempted killing.

If, after release, you knowingly fail to appear as the conditions of release require, or to surrender to serve a sentence, you may be prosecuted for failing to appear or surrender and additional punishment may be imposed. If you are convicted of:

- (1) an offense punishable by death, life imprisonment, or imprisonment for a term of fifteen years or more – you will be fined not more than \$250,000 or imprisoned for not more than 10 years, or both;
- (2) an offense punishable by imprisonment for a term of five years or more, but less than fifteen years – you will be fined not more than \$250,000 or imprisoned for not more than five years, or both;
- (3) any other felony – you will be fined not more than \$250,000 or imprisoned not more than two years, or both;
- (4) a misdemeanor – you will be fined not more than \$100,000 or imprisoned not more than one year, or both.

A term of imprisonment imposed for failure to appear or surrender will be consecutive to any other sentence you receive. In addition, a failure to appear or surrender may result in the forfeiture of any bond posted.

**Acknowledgment of the Defendant**

I acknowledge that I am the defendant in this case and that I am aware of the conditions of release. I promise to obey all conditions of release, to appear as directed, and surrender to serve any sentence imposed. I am aware of the penalties and sanctions set forth above.

Defendant's Signature

City and State

**Directions to the United States Marshal**

- ( ☒ ) The defendant is ORDERED released after processing.
- ( ☐ ) The United States marshal is ORDERED to keep the defendant in custody until notified by the clerk or judge that the defendant has posted bond and/or complied with all other conditions for release. If still in custody, the defendant must be produced before the appropriate judge at the time and place specified.

Date: 7/19/2011

Judicial Officer's Signature

Printed name and title

DISTRIBUTION: COURT DEFENDANT PRETRIAL SERVICE U.S. ATTORNEY U.S. MARSHAL

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

Criminal No.  
11-10260-NMG

UNITED STATES OF AMERICA

v.

AARON SWARTZ

**INITIAL SCHEDULING ORDER**

July 19, 2011

DEIN, M.J.

The above named defendant having been arraigned before this court on Tuesday, July 19, 2011, and having elected to proceed under the automatic discovery rules, IT IS HEREBY ORDERED in accordance with Local Rules (LR) 116.1 through 116.5 that:

- A. Any discovery request letters shall be sent and filed by Tuesday, August 30, 2011. See LR 116.3(A) and (H).
- B. Any responses to discovery request letters shall be sent and filed within fourteen (14) days of receipt of the discovery request letter(s) referred to in Paragraph A immediately above, or on or before Tuesday, September 13, 2011, **whichever date shall first occur**. See LR 116.3(A).
- C. Any and all discovery motions shall, consistent with the provisions of LR 116.3(E) through 116.3(H), be filed on or before 14 days after receipt of the opposing party's declination to provide the requested discovery, **or** 14 days after the opposing party has received the discovery request letter

and has failed to respond thereto, **whichever date shall first occur**. See LR 116.3(E) and (H).

- D. Response(s) to any motions shall be filed on or before fourteen (14) days after motions have been filed consistent with the provisions of Paragraph C immediately above. See LR 116.3(I).
- E. In the event that a defendant notifies the attorney for the government that the defendant intends to offer a plea of guilty, the attorney for the government shall forthwith notify this court of that fact by writing indicating the date that that notification was made to the attorney for the government.
- F. **An Initial Status Conference in accordance with LR 116.5 will be held on Friday, September 9, 2011, at 10:00 a.m., in Courtroom No. 15 on the Fifth Floor.**<sup>1</sup>
- G. **A joint memorandum addressing those items set forth in Local Rule 116.5(A)(1) through Local Rule 116.5(A)(7) shall be filed on or before the close of business, Friday, September 2, 2011.**

/ s / Judith Gail Dein  
JUDITH GAIL DEIN  
United States Magistrate Judge

---

<sup>1</sup> Defendants are not required to be present at the Initial Status Conference. Inasmuch as this court concludes that the Initial Status Conference is not a critical proceeding within the meaning of Rule 43, F.R. Crim. P., defendants in custody will **not** be transported to court for the Initial Status Conference absent a showing of exceptional cause on motion duly filed in advance of the Initial Status Conference, See 43(c)(3), F.R. Crim. P.

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

Criminal No.  
11-10260-NMG

UNITED STATES OF AMERICA

v.

AARON SWARTZ

**ORDER ON EXCLUDABLE TIME**

July 19, 2011

DEIN, M.J.

The defendant having elected to proceed under the Automatic Discovery Rules in accordance with Local Rules 116.1 through 116.5, the indictment in this case having been made public on Tuesday, July 19, 2011, and the defendant having appeared for the initial appearance on Tuesday, July 19, 2011 and having been arraigned on Tuesday, July 19, 2011, this court finds and concludes pursuant to the provisions of 18 U.S.C. § 3161(h)(7)(A) and Section 5(b)(7)(b) of the Plan for Prompt Disposition of Criminal Cases in the United States District Court for the District Court for the District of Massachusetts (Statement of Time Limits Adopted by the Court and Procedures for Implementing Them, effective December 2008), as follows:

That the interests of justice, *i.e.*, to provide the parties additional time to develop their respective discovery plans and produce discovery under the Automatic Discovery Rules in accordance with Local Rules 116.1 through 116.5, outweighs the best interests of the public and the defendant for a trial within seventy days of the return of an indictment or filing of an information. Therefore, it is hereby ORDERED that the Clerk of this Court enter excludable time

in the amount of twenty-eight (28) days,<sup>1</sup> commencing Tuesday, July 19, 2011, the date of the arraignment herein, and concluding Tuesday, August 16, 2011.<sup>2</sup> See Local Rule 112.2(A)(2).

/ s / Judith Gail Dein  
JUDITH GAIL DEIN  
United States Magistrate Judge

---

<sup>1</sup> This court further finds it to be in the interests of justice that, under Local Rule 112.2(A)(3), an additional order of excludable time in the amount of fourteen (14) days be entered upon the filing of a letter requesting discovery under Local Rule 116.3(A), so that the responding parties may appropriately develop their responses thereto. Absent further order of this court on motion duly filed, that additional order shall be deemed in effect and effective without the need of a further written order by this court on the date that a letter requesting discovery under Local Rule 116.3(A) is filed.

<sup>2</sup> The parties are hereby advised that under the provisions of Rule 2(b) of the Rules for United States Magistrates in the United States District Court for the District of Massachusetts, any party may move for reconsideration by a district judge of the determination(s) and order(s) set forth herein within fourteen (14) days after receipt of a copy of this order, unless a different time is prescribed by this court or the district judge. The party seeking reconsideration shall file with the Clerk of this Court, and serve upon all parties, a written notice of the motion which shall specifically designate the order or part thereof to be reconsidered and the basis for the objection thereto. The district judge, upon timely motion, shall reconsider the magistrate judge's order and set aside any portion thereof found to be clearly erroneous in fact or contrary to law. The parties are further advised that the United States Court of Appeals for this Circuit has indicated that failure to comply with this rule shall preclude further appellate review. See Keating v. Secretary of Health and Human Services, 848 F.2d 271 (1st Cir. 1988); United States v. Emiliano Valencia-Copete, 792 F.2d 4 (1st Cir. 1986); Park Motor Mart, Inc. v. Ford Motor Co., 616 F.2d 603 (1st Cir. 1980); United States v. Vega, 678 F.2d 376, 378-379 (1st Cir. 1982); Scott v. Schweiker, 702 F.2d 13, 14 (1st Cir. 1983); see also, Thomas v. Arn, 474 U.S. 140, 106 S. Ct. 466 (1985).



UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

<b>UNITED STATES OF AMERICA</b>	)	
	)	
<b>v.</b>	)	<b>Criminal No. 11-CR-10260-NMG</b>
	)	
<b>AARON SWARTZ,</b>	)	
Defendant	)	

GOVERNMENT'S LOCAL RULE 112.4(B)  
ORGANIZATIONAL VICTIM DISCLOSURE STATEMENT

The United States hereby notifies the Court, as required by Local Rule 112.4(B), that it has identified the entities listed below as organizational victims, parent companies of victims, or publicly held corporations that own 10% or more of victim companies, of the crimes alleged in the above-captioned indictment:

Massachusetts Institute of Technology

JSTOR

ITHAKA

In addition there are several hundred publishers, on whose behalves JSTOR made academic journals available for purchase by the public. The government will obtain a list of these publishers for the Court from JSTOR at the Court's request.

Respectfully submitted,

CARMEN M. ORTIZ  
United States Attorney

By: /s/ Stephen P. Heymann  
Stephen P. Heymann  
Scott Garland  
Assistant U.S. Attorneys

Dated: July 20, 2011

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/s/ Stephen P. Heymann  
Stephen P. Heymann  
Assistant United States Attorney

Date: July 20, 2011

UNITED STATES DISTRICT COURT FOR THE  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA

v.

AARON SWARTZ,

Defendant

CRIMINAL No. 11-CR-10260-NMG

NOTICE OF APPEARANCE FOR  
ASSISTANT UNITED STATES ATTORNEY SCOTT L. GARLAND

Assistant United States Attorney Scott L. Garland will be representing the United States as counsel for the government in this matter, in addition to Assistant United States Attorney Stephen P. Heymann.

Respectfully submitted,

CARMEN M. ORTIZ  
United States Attorney

By: /s/ Scott L. Garland  
SCOTT L. GARLAND  
Assistant United States Attorney

CERTIFICATE OF SERVICE

I certify that this document was filed on the date listed below through the ECF system, which will provide electronic notice to counsel as identified on the Notice of Electronic Filing.

/s/ Scott L. Garland  
Scott L. Garland  
Assistant United States Attorney

Dated: July 20, 2011

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	Criminal No. 11-CR-10260
	)	
	)	M.J. /Court Nos. 11m-5013-JGD,
v.	)	11m-5014-JGD, 11m-5015-JGD,
	)	11m-5031-JGD, 11m-5061-JGD,
AARON SWARTZ,	)	11m5062-JGD, 11m-5063-JGD,
Defendant	)	11m-5143-JGD, and 11m-5138-JGD

**MOTION TO UNSEAL SEARCH WARRANTS,  
ASSET FORFEITURE SEIZURE WARRANT, AND SUPPORTING APPLICATIONS**

The United States of America hereby moves this Court to direct that the Search Warrants, Asset Forfeiture Seizure Warrant and supporting Applications be unsealed in the following matters for the limited purpose of providing copies to the defendant and the Middlesex District Attorney's Office: M.J./Court Nos. 11m-5013-JGD, 11m-5014-JGD, 11m-5015-JGD, 11m-5031-JGD, 11m-5061-JGD, 11m5062-JGD, 11m-5063-JGD, 11m-5143-JGD and 11m-5138-JGD.

In support of this motion, the government states that the defendant surrendered to an arrest warrant on July 19, 2011. The government seeks to provide these materials to the defendant as part of automatic discovery. In addition, the government has been asked by the Middlesex District Attorney's Office to make these materials available to it, as they contain facts potentially material to a criminal matter pending in Middlesex County regarding the defendant.

Government counsel has conferred with defense counsel pursuant to Local Rule 7.2(a)(2), and defense counsel assents to the limited unsealing sought herein.

Respectfully submitted,

CARMEN M. ORTIZ  
United States Attorney

By: /s/ Stephen P. Heymann  
Stephen P. Heymann  
Scott L. Garland  
Assistant U.S. Attorneys

Date: July 21, 2011

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) .

/s/ Stephen P. Heymann  
Stephen P. Heymann  
Assistant United States Attorney

Date: July 21, 2011

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	Criminal No. 11-CR-10260-NMG
AARON SWARTZ,	)	
	)	
Defendant.	)	

**MOTION BY UNITED STATES FOR AUTHORIZATION TO USE  
ALTERNATIVE NOTICE PROCEDURES FOR VICTIMS**

The United States of America, by and through its undersigned attorney, respectfully requests authorization to use alternative notice procedures for the large number of actual and potential victims in the instant case.

The Justice for All Act of 2004 (“the Act”), codified at 18 U.S.C. § 3771, was signed into law on October 30, 2004. The Act provides certain rights to victims in federal criminal proceedings. Among these rights are the right to “reasonable, accurate, and timely notice” of public court proceedings. 18 U.S.C. § 3771(a). The Act defines a crime victim as “a person directly and proximately harmed as a result of the commission of a Federal offense ...” 18 U.S.C. § 3771(e). Importantly, the Act recognizes that for crimes involving multiple victims, the Court has discretion to adopt procedures that will not unduly interfere with the criminal proceedings. Thus, 18 U.S.C. § 3771(d)(2) provides:

[i]n a case where the Court finds that the number of crime victims makes it impracticable to accord all of the crime victims the rights described in subsection (a), the Court shall fashion a reasonable procedure to give effect to this chapter that does not unduly complicate or prolong the proceedings.

There are two classes of victims in the present case. First, there are those entities whose computer systems were compromised by the defendant: the Massachusetts Institute of Technology (“MIT”) and JSTOR (owned by ITHAKA). Second, there are the numerous publishers for whom JSTOR facilitated the sale of individual articles stored in JSTOR’s archive.

The government does not seek a complete waiver of the notice provision of the Act. Rather, the United States proposes that the Court authorize that notification be made to victims in the following manner:

- a. Department of Justice Victim Notification System: The government will utilize the Victim Notification System (VNS) to notify JSTOR and MIT. The VNS enables the government to inform victims entered in the system of scheduled court dates and significant court event outcomes.
- b. Website: The government will place links on its website ([www.usdoj.gov/usao/ma](http://www.usdoj.gov/usao/ma)) to provide information to interested publishers and the public regarding this case.

In this case, the number of publishers affected was large, and as noted above, it is impracticable to provide individualized notice to all of them. The procedure described above is a reasonable one that will give effect to the Act without unduly complicating or prolonging the proceedings.



WHEREFORE, the United States respectfully requests that the Court authorize the government to enact the proposed plan for notifying victims of this crime, and that the Court find that the proposed plan is a reasonable procedure to satisfy the government's obligations under 18 U.S.C. § 3771.

Very truly yours,

MICHAEL J. SULLIVAN  
United States Attorney

By: /s/ Stephen P. Heymann  
STEPHEN P. HEYMANN  
Assistant U.S. Attorney

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/s/ Stephen P. Heymann  
STEPHEN P. HEYMANN  
Assistant United States Attorney

Date: July 21, 2011

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:3986281@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Order on Motion for Miscellaneous Relief  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 8/2/2011 at 12:40 PM EDT and filed on 7/27/2011

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** No document attached

**Docket Text:**

**Ch. Magistrate Judge Judith G. Dein: ELECTRONIC ORDER entered granting [11] Motion as to Aaron Swartz (1) The US Attorney's Office is responsible to provide copies to the defendant and Middlesex District Attorney's Office. (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Stephen P. Heymann Stephen.Heymann@usdoj.gov, janet.smith@usdoj.gov, usama.ecf@usdoj.gov

Andrew Good agood@goodcormier.com, hill@goodcormier.com, josh@goodcormier.com,  
lpetrova@goodcormier.com, pcormier@goodcormier.com

Scott Garland scott.garland@usdoj.gov, janet.smith@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:3986289@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Order on Motion for Victim Rights  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 8/2/2011 at 12:42 PM EDT and filed on 7/27/2011

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** No document attached

**Docket Text:**

**Ch. Magistrate Judge Judith G. Dein: ELECTRONIC ORDER entered granting [12] Motion for Victim Rights as to Aaron Swartz (1); granting [12] Motion as to Aaron Swartz (1) (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Stephen P. Heymann Stephen.Heymann@usdoj.gov, janet.smith@usdoj.gov, usama.ecf@usdoj.gov

Andrew Good agood@goodcormier.com, hill@goodcormier.com, josh@goodcormier.com,  
lpetrova@goodcormier.com, pcormier@goodcormier.com

Scott Garland scott.garland@usdoj.gov, janet.smith@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

**UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS**

<b>UNITED STATES OF AMERICA</b>	)	
	)	
v.	)	<b>Criminal No. 11-CR-10260-NMG</b>
	)	
<b>AARON SWARTZ,</b>	)	
	)	
<b>Defendant</b>	)	

**MOTION FOR ORDER OF EXCLUDABLE DELAY**  
**PURSUANT TO THE SPEEDY TRIAL ACT**

The United States of America, by and through Assistant United States Attorney Stephen Heymann, moves for an order designating the period from August 16, through and including September 9, as excludable delay pursuant to the Speedy Trial Act, 18 U.S.C. §3161(h)(7)(A), on the grounds that the ends of justice served by granting the requested continuance of time outweigh the best interests of the public and the defendant in a speedy trial. The government further asks this Court to issue the attached proposed Order of Excludable Delay. In support of this request, the government states as follows:

1. The discovery materials contain potentially sensitive, confidential and proprietary communications, documents, and records obtained from JSTOR and MIT, who are alleged in the indictment to be victims. The parties are presently determining whether they can agree on the terms of a protective order for these records, or whether the issue will need to be litigated here before discovery can continue further. In addition, this case involves material computer logs and computer programs. The government anticipates that the defendant will need a period of additional time in which to: (a) review discovery produced by the government; (b) investigate the evidence and

possible defenses; and (c) evaluate the need for, and to prepare, motions to dismiss, suppress, and other pre-trial motions.

2. The government asks the Court to enter an order excluding from the speedy trial computation the period from August 16, 2011 through and including September 9, 2011. This period constitutes “reasonable time necessary for effective preparation, taking into account the exercise of due diligence,” and that the ends of justice served by granting the continuance outweigh the best interest of the public and the defendant in a speedy trial pursuant to the Speedy Trial Act, 18 U.S.C. §§3161(h)(7)(A) and 3161(h)(7)(B).

3. Government counsel has conferred with defense counsel concerning the relief sought by this motion. Defense counsel has indicated that he intends to file a prompt response to the motion.

Respectfully submitted

CARMEN M. ORTIZ  
UNITED STATES ATTORNEY

Date: August 16, 2011

By: /s/ Stephen P. Heymann  
STEPHEN P. HEYMANN  
SCOTT L. GARLAND  
Assistant U.S. Attorney

CERTIFICATE OF SERVICE

I hereby certify that the foregoing document filed through the ECF system will be sent electronically to counsel for Defendant, who is a registered participant as identified on the Notice of Electronic Filing (NEF).

Date: August 16, 2011

/s/ Stephen P. Heymann  
STEPHEN P. HEYMANN  
Assistant U.S. Attorney

**UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS**

<b>UNITED STATES OF AMERICA</b>	)	
	)	
<b>v.</b>	)	<b>Criminal No. 11-CR-10260-NMG</b>
	)	
<b>AARON SWARTZ,</b>	)	
	)	
<b>Defendant</b>	)	

**ORDER OF EXCLUDABLE DELAY**

Upon consideration of the government's motion seeking an order of excludable delay, the Court finds as follows:

1. A continuance of this proceeding from August 16, 2011 through and including September 9, 2011 is necessary to ensure that the parties have time to seek to develop, and that a proposed protective order governing discovery be presented to this Court, and that counsel for the defendant and the defendant have sufficient time to review discovery, investigate the evidence, consider whether to file pretrial motions, and then to prepare any such pretrial motions. I find, given the specific circumstances in this case, that this continuance constitutes "reasonable time necessary for effective preparation, taking into account the exercise of due diligence," 18 U.S.C. §3161(h)(7)(B).

3. The ends of justice served by granting the continuance from August 16, 2011 through and including September 9, 2011 outweigh the best interest of the public and the defendant in a speedy trial pursuant to the Speedy Trial Act, 18 U.S.C. §§3161(h)(7)(A) and 3161(h)(7)(B).

Accordingly, the Court hereby grants the government's motion and **ORDERS** that the period from August 16, 2011 through and including September 9, 2011 be excluded from the Speedy Trial Act computation of the time within which trial in the case must begin, pursuant to 18 U.S.C. §§3161(h)(7)(A) and 3161(h)(7)(B).

---

**JUDITH G. DEIN**  
**CHIEF U. S. MAGISTRATE JUDGE**

Dated: \_\_\_\_\_



UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF  
AMERICA

v.

AARON SWARTZ,  
Defendant.

CRIMINAL No. 11-CR-10260-NMG

JOINT MEMORANDUM FOR INITIAL STATUS CONFERENCE

The parties submit this joint memorandum addressing the issues set out in Local Rule 116.5(A).

(1) Relief from Rule 116.3 – Discovery Motion Practice

The parties request relief from the schedule set out in Local Rule 116.3 in view of the parties' dispute concerning a protective order.

(2) Expert witness discovery

The government anticipates offering expert witness testimony in the areas of computer networks, computer network security, computer programming, computer forensics, records created by computers and attempts to breach computer network security measures. The defendant requests discovery concerning expert witnesses. The parties disagree on what dates should be established for expert disclosure and whether the dates should be the same for both parties.

(3) Additional discovery

The government has initiated automatic discovery required under the Local Rules but has conditioned providing some of this discovery subject to entry of a protective order, the terms of

which the parties are currently negotiating. If the parties cannot reach agreement, the government will file a motion for a protective order and the defendant will file a motion to compel disclosure in the absence of a protective order or proposing different terms for a protective order. The parties' cross-motions will be no later than two weeks after the September 9, 2011 status conference.

Defense counsel will need more time to review the material already provided and the material that will be provided after entry of a protective order. The government anticipates obtaining other discoverable items and will provide them to defense counsel or make them available for inspection when available.

(4) Motion date

The government contends that a protective order is appropriate in this case. The parties have not yet determined whether they can agree on the terms of a protective order or whether this issue will need to be litigated. The parties request that the Court order the parties' cross-motions for a protective order and to compel discovery be filed no later than two weeks after the September 9<sup>th</sup> status conference, and set the motions for hearing four weeks after the status conference.

The parties request that the Court schedule an interim status conference, at which the Court would establish the date by which Defendant would be required to file any motions to dismiss the indictment or to suppress evidence.

(5) Excludable delay

The parties ask the Court to grant the government's previously-filed motion to exclude the time from August 16, 2011, through September 9, 2011, and to exclude this time and the time from the date of the Initial Status Conference to an interim status conference under the Speedy Trial Act, 18 U.S.C. § 3161(h)(7)(A), for the parties to negotiate a protective order, and for Defendant Swartz

to review discovery, investigate possible defenses, and evaluate the need for pre-trial motions. The ends of justice served by this exclusion would outweigh the best interest of the public and the defendant in a speedy trial.

(6) Trial likelihood and length:

The parties anticipate that there will be a trial and that it will take approximately two weeks, but will likely take longer if the parties are unable to work out trial stipulations and if Defendant Swartz puts on any witnesses in his defense.

(7) Interim status conference:

The parties ask the Court to schedule an interim status conference during the week of October 3, 2011.

Respectfully submitted,

CARMEN M. ORTIZ  
United States Attorney

By: /s/ Scott L. Garland  
Stephen P. Heymann  
Scott L. Garland  
Assistant U.S. Attorneys

Andrew Good, Esq.  
Counsel for Defendant Aaron Swartz

/s/ Andrew Good by slg  
Andrew Good, Esq.  
Good and Cormier

Date: September 7, 2011

CERTIFICATE OF SERVICE

I hereby certify that this document is being filed through the ECF system and will therefore be sent electronically to the registered participants as identified on the Notice of Electronic Filing.

/s/ Scott L. Garland  
Scott L. Garland  
Assistant United States Attorney

Date: September 7, 2011

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES	)	
OF AMERICA	)	
	)	
v.	)	Crim. No. 11-CR-10260-NMG
	)	
AARON SWARTZ,	)	
Defendant.	)	

DEFENDANT'S MOTION FOR LEAVE TO CHANGE RESIDENTIAL ADDRESS

Aaron Swartz moves this Court for leave to change his residential address to 76 Oxford St # 1, Cambridge, MA 02138-1809. Mr. Swartz has already reported this change to Pretrial Services Officer Gina Affsa. The residential change is necessary because his former landlord would not extend his lease on his Massachusetts Avenue apartment.

As reported at the arraignment, Mr. Swartz has begun working as independent contractor performing research for a New York City company. This work requires Mr. Swartz to spend variable days of the week in New York City. When he stays over night in New York, Mr. Swartz's address is 99 Graham Street, Apt. #1, Brooklyn, New York 11206.

Mr. Swartz reports in person weekly to the Pretrial Services office in Boston.

Respectfully submitted,

/s/Andrew Good  
Andrew Good  
BBO # 201240  
Good & Cormier  
83 Atlantic Avenue  
Boston, MA 02110  
Tel. 617-523-5933  
agood@goodcormier.com

CERTIFICATE OF SERVICE

I hereby certify that the foregoing document filed through the ECF system will be sent to counsel for the government who are registered participants as identified on the Notice of Electronic Filing (“NEF”).

DATED: September 8, 2011

/s/ Andrew Good  
Andrew Good

G:\CLIENTS\Swartz, Aaron\Pleadings - Federal Court Case\Motion For Leave to Change Residential Address.doc



MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4039555@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Status Conference by Magistrate Judge  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 9/12/2011 at 5:08 PM EDT and filed on 9/9/2011

**Case Name:** USA v. Swartz  
**Case Number:** 1:11-cr-10260-NMG  
**Filer:**  
**Document Number:** No document attached

**Docket Text:**

**ELECTRONIC Clerk's Notes for proceedings held before Ch. Magistrate Judge Judith G. Dein: Status Conference as to Aaron Swartz held on 9/9/2011; Counsel report current case status and seek further conference for 11/2/11 @ 2:30pm. Motion hearing is set for 10/11/11 @ 11:00am. (Attorneys present: Garland, Heymann and Good. )Court Reporter Name and Contact or digital recording information: Digital Recording. (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Andrew Good agood@goodcormier.com, hill@goodcormier.com, josh@goodcormier.com, lpetrova@goodcormier.com, pcormier@goodcormier.com

Scott Garland scott.garland@usdoj.gov, janet.smith@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

CRIMINAL No.  
11-10260-NMG

UNITED STATES OF AMERICA  
v.

AARON SWARTZ

**ORDER AND  
INITIAL STATUS REPORT**

September 9, 2011

DEIN, M.J.

An Initial Status Conference was held before this court on Friday, September 9, 2011 pursuant to the provisions of Local Rule 116.5(A). Based on that conference, this court enters the following report and orders, to wit:

1. The defendant is in the process of reviewing the materials produced by the government to date. The parties are attempting to agree on the terms of a confidentiality agreement to govern the terms of production of additional documents. If the parties cannot agree, they shall each file their proposed order by **September 27, 2011**; responses are to be filed by **October 6, 2011**, and argument will be heard on **October 11, 2011 at 11:00 a.m.**
2. The defendant has requested expert discovery, and the parties will submit a proposed schedule at the next status conference. Pursuant to the schedule, the government shall produce its expert discovery first, then the defendant, then an opportunity for the government to respond.
3. All dates for filing discovery and/or dispositive motions shall be set at the next status conference.
4. In this court's view, this is not a case involving unusual or complex issues for which an early joint conference of the district judge and the magistrate judge with counsel of record would be useful.
5. In this court's view, this is not a case involving features which would warrant special attention or modification of the standard schedule, except as provided herein.

6. The parties anticipate that there will be a trial, and that the government's case will take approximately 2 weeks.
7. This court finds and concludes, pursuant to the provisions of 18 U.S.C. § 3161(h)(7)(A) and Section 5(b)(7)(B) of the Plan for Prompt Disposition of Criminal Cases in the United States District Court for the District of Massachusetts (Statement of Time Limits Adopted by the Court and Procedures for Implementing Them, Effective December 2008) that the defendant requires additional time for the preparation of an effective defense, including time for review of the evidence, and consideration of alternatives concerning how best to proceed with this matter, and that the interests of justice outweighs the best interests of the public and the defendant for a trial within seventy days of the return of an indictment.

Accordingly, it is hereby ordered that the Clerk of this Court enter excludable time for the period of August 16, 2011 through November 2, 2011, that being the period between the expiration of the last order on excludable time and the next status conference.<sup>1</sup>

8. Based upon the prior order of the court dated July 19, 2011 and the order entered contemporaneously herewith, at the time of the Interim Status Conference on November 2, 2011 there will be zero (0) days of non-excludable time under the Speedy Trial Act and seventy (70) days will remain under the Speedy Trial Act in which this case must be tried.
9. **An Interim Status Conference has been scheduled for November 2, 2011 at 2:30 p.m. Counsel for the respective parties shall file a Joint Memorandum addressing the matters set forth in LR 116.5(A)(1) through (7) before the close of business no less than THREE business days prior to that Status Conference. In addition, the parties shall include in the Joint Memorandum not only the periods**

---

<sup>1</sup> The parties are hereby advised that under the provisions of Rule 2(b) of the Rules for United States Magistrates in the United States District Court for the District of Massachusetts, any party may move for reconsideration by a district judge of the determination(s) and order(s) set forth herein within ten (10) days after receipt of a copy of this order, unless a different time is prescribed by this court or the district judge. The party seeking reconsideration shall file with the Clerk of this Court, and serve upon all parties, a written notice of the motion which shall specifically designate the order or part thereof to be reconsidered and the basis for the objection thereto. The district judge, upon timely motion, shall reconsider the magistrate's order and set aside any portion thereof found to be clearly erroneous in fact or contrary to law. The parties are further advised that the United States Court of Appeals for this Circuit has indicated that failure to comply with this rule shall preclude further appellate review. See Keating v. Secretary of Health and Human Services, 848 F.2d 271 (1<sup>st</sup> Cir. March 31, 1988); United States v. Emiliano Valencia-Copete, 792 F.2d 4 (1<sup>st</sup> Cir. 1986); Park Motor Mart, Inc. v. Ford Motor Co., 616 F.2d 603 (1<sup>st</sup> Cir. 1980); United States v. Vega, 678 F.2d 376, 378-379 (1<sup>st</sup> Cir. 1982); Scott v. Schweiker, 702 F.2d 13, 14 (1<sup>st</sup> Cir. 1983); see also Thomas v. Arn, 474 U.S. 140, 106 S. Ct. 466 (1985).

**of excludable time that are applicable, but also the amount of time remaining under the Speedy Trial Act before trial must commence, as well as the total amount of time which has been excluded.**

/ s / Judith Gail Dein  
JUDITH GAIL DEIN  
UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

CRIMINAL No.  
11-10260-NMG

UNITED STATES OF AMERICA

v.

AARON SWARTZ

**ORDER ON EXCLUDABLE TIME**

September 9, 2011

DEIN, M.J.

With the agreement of the parties, this court finds and concludes, pursuant to the provisions of 18 U.S.C. § 3161(h)(7)(A) and Section 5(b)(7)(B) of the Plan for Prompt Disposition of Criminal Cases in the United States District Court for the District of Massachusetts (Statement of Time Limits Adopted by the Court and Procedures for Implementing Them, Effective December 2008) that the defendant requires additional time for the preparation of an effective defense, including time for review of the evidence, preparation of motions and consideration of alternatives concerning how best to proceed, and that the interests of justice outweighs the best interests of the public and the defendant for a trial within seventy days of the return of an indictment, and that not granting this continuance would deny counsel for the defendant a reasonable time necessary for effective preparation. See 18 U.S.C. § 3161(h)(7)(B)(iv).

Accordingly, it is hereby ordered that the Clerk of this Court enter excludable time for the period of

August 16, 2011 through November 2, 2011,

that being the period between the expiration of the last order on excludable time and the next status conference.

Based upon the prior order of the court dated July 19, 2011 and this order, at the time of the Interim Status Conference on November 2, 2011 there will be zero (0) days of non-excludable time under the Speedy Trial Act and seventy (70) days will remain under the Speedy Trial Act in which this case must be tried.

/ s / Judith Gail Dein  
JUDITH GAIL DEIN  
United States Magistrate Judge

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4050407@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Order on Motion for Miscellaneous Relief  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 9/20/2011 at 9:47 AM EDT and filed on 9/20/2011

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** No document attached

**Docket Text:**

**Ch. Magistrate Judge Judith G. Dein: ELECTRONIC ORDER entered granting [15] Motion Change Residential Address as to Aaron Swartz (1) (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Andrew Good agood@goodcormier.com, hill@goodcormier.com, josh@goodcormier.com,  
lpetrova@goodcormier.com, pcormier@goodcormier.com

Scott Garland scott.garland@usdoj.gov, janet.smith@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**



**UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS**

**UNITED STATES OF AMERICA**

**v.**

**AARON SWARTZ,  
Defendant**

)  
)  
)  
)  
)  
)

**Criminal No. 11-10260-NMG**

**MOTION OF THE UNITED STATES FOR A PROTECTIVE ORDER**

The United States moves the Court to enter the attached protective order. The order is necessary to protect victims in the case from the very real risk of serious and irreparable harm while permitting the effective production of additional materials pursuant to Fed. R. Crim. P. 16 and the Local Rules of this Court.

As the Court is aware, Aaron Swartz is charged with illegally accessing MIT's computer network and, through it, stealing a major portion of JSTOR's valuable digital database. While some peripheral facts will likely be disputed at trial, much of the evidence that cannot be disputed (university records, computer logs, records from one of Swartz's own computers, and surveillance camera recordings) demonstrate that Swartz:

1. was not a student, faculty member or employee of MIT;
2. gained physical access to MIT's computer network through a laptop computer he had installed in a restricted wiring closet in the basement of a research building;
3. intentionally masked his face with a bicycle helmet to avoid identification on a video camera as he entered the closet to remove the laptop;
4. used fictitious names and manipulated computer identification information to get and maintain access to MIT's computer network;

5. took repeated and affirmative steps to evade efforts by both MIT and JSTOR to lock him out of their computer networks;
6. downloaded a major portion of JSTOR's valuable digital database of scientific journals over the course of three months; and
7. earlier posted on one of his websites, guerrillaopenaccess.com, a call-to-arms entitled "Guerrilla Open Access *Manifesto*" which concluded "We need to download scientific journals and upload them to file sharing networks. We need to fight for *Guerrilla Open Access*." (Emphasis in the original.)

In this context, Aaron Swartz cannot be entrusted with responsibly protecting confidential internal records of MIT and JSTOR. These include databases, private electronic communications and records that are either very valuable or that could cause great damage if released to the public:

1. several million JSTOR articles that Swartz downloaded;
2. a software program Swartz used during his automated theft from JSTOR (and a variant of it);
3. discussion and analyses of Swartz's illegal access to MIT's network and possible means to defend against it;
4. analyses of methods used by Swartz during his automated theft from JSTOR and internal discussions on possible ways to stop it; and
5. descriptions of the networks' and databases' vulnerabilities.

The United States does not seek to withhold discovery of these items from Defendant or his defense counsel. Quite the contrary. The United States wants to produce this material, in many cases well ahead of the deadlines set by statute and the Local Rules. The proposed protective order, however, is critically necessary to prevent irreparably harmful redistribution of the material, whether intentional or unintentional.

The government's protective order proposes two levels of protection. The greatest is accorded the extensive database of digitized scientific articles that Defendant downloaded with his automated attack. These articles are JSTOR's lifeblood. JSTOR has spent millions of dollars to locate articles, work out copyright deals, digitize the articles, store them, and make them available online.<sup>1</sup> Accordingly, these articles should be protected by being maintained at government offices. The government can secure this data to an extent that a law office cannot. If and when the defense wishes to examine it, the government will make a copy available for examination with the assistance of an agent otherwise uninvolved in the case, who will be instructed not to communicate with the prosecution team about what items the defense reviews except at the request of the defendant or with prior approval of the Court. (The government does not expect the defense counsel, experts, or investigators to mishandle the evidence, whether at the government's offices or at their own. Rather, the government proposes to keep the articles in the government's custody because they will be safest there, including from unrelated third parties who might wish to access them.)

An important but less restrictive protection is accorded to the rest of the discovery materials, including the confidential records of victims MIT and JSTOR, Swartz's programs for downloading articles, and analyses of downloading methods or network vulnerabilities. Copies of these would be provided to defense counsel, but their custody would be limited to his office and the office of whichever experts and investigators that Defendant might retain. Defendant himself could review these materials at their offices and under their supervision.

---

<sup>1</sup>A JSTOR representative will address this issue before the Court at the hearing on this motion.

The government's protective order would not unfairly impede Defendant's ability to assist in the preparation of his defense. The United States does not seek to limit these discovery materials to his attorneys' eyes only. Rather, Defendant could review the materials at a variety of locations: the offices of his defense counsel, his expert witnesses, or his private investigators. Just as the United States did not oppose Defendant's bid to move outside the District, the United States does not seek to limit the geographic location of his attorneys, experts, or investigators that he hires, nor their number. But limiting his contact and review of these records to those custodians' offices is necessary. In a case that involves sensitive information, Defendant can be expected to go through reasonable security measures to access that information.

The United States' proposal is reasonable: you don't put a multimillion dollar database and discussions of its vulnerabilities in the custody of the person accused of stealing it.

If the Court seeks to compromise by asking the United States to cull through the discovery materials and designate page by page which documents would be stored with defense counsel and which with Defendant, the United States will comply.<sup>2</sup> But doing so would seriously delay production. There are a lot of pages to go through page-by-page. Rather, the United States would prefer to disclose its discovery early. The government's protective order would allow this early discovery.

For these reasons, the United States moves the Court to enter the attached protective order.

---

<sup>2</sup>The protective order already specifies an easily definable subset of documents that Defendant could store at his residence: fingerprint analyses, photo spreads, search warrants and supporting affidavits.

Respectfully submitted,

Carmen M. Ortiz  
United States Attorney

By: /s/ Scott L. Garland  
Stephen P. Heymann  
Scott L. Garland  
Assistant U.S. Attorneys

CERTIFICATE OF SERVICE

I hereby certify that these documents are being filed through the ECF system and therefore will be sent electronically to the registered participants as identified on the Notice of Electronic Filing.

/s/ Scott L. Garland  
Scott L. Garland  
Assistant U.S. Attorney

Date: September 27, 2011

**UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS**

<b>UNITED STATES OF AMERICA</b>	)	
	)	
<b>v.</b>	)	<b>Criminal No. 11-10260-NMG</b>
	)	
<b>AARON SWARTZ,</b>	)	
<b>Defendant</b>	)	

**PROTECTIVE ORDER**

Whereas the Indictment in this case alleges that JSTOR and the Massachusetts Institute of Technology ("MIT") are victims of conduct committed by Defendant Aaron Swartz, and the materials discoverable in this case under Fed. R. Crim. P. 16 and L. R. 116.1-116.2 contain potentially sensitive, confidential and proprietary communications, documents, and records obtained from JSTOR and MIT, including discussion of the victims' computer systems and security measures,

The Court finds good cause for, entry of this Protective Order pursuant to Fed. R. Crim. P. 16(d):

1. The Government shall produce all documents, files and records discoverable under Fed. R. Crim. P. 16 and L.R. 116.1-116.2 for review by the defense - that is, Defendant Swartz, his defense counsel and their staff, and any experts or investigators retained by the defense - in accordance with the conditions set by this Order.

2. With the exception of files contained on four hard drives delivered to the Government pursuant to an agreement between JSTOR and Defendant Swartz dated June 4, 2011, and "Downloaded Data" as defined in that agreement contained on a Maxtor hard drive

seized by the Government on January 6, 2011, defense counsel, their staff, and experts or investigators retained by the defense may obtain and make copies of discovery materials they deem necessary to prepare the defense of this case. All discovery materials and copies of discovery materials made by them or provided to them by the United States shall be kept securely at the offices of defense counsel, retained experts, or retained investigators, and shall not be transmitted to or kept anywhere else. Notwithstanding the foregoing, Defendant may keep securely at his residence in Boston or New York copies of the fingerprint analyses, photo spreads, search warrants and supporting affidavits produced during discovery for the purpose of litigating this case.

3. The defense shall use the discovery materials solely and exclusively to litigate this case (including investigation, pre-trial motions, trial preparation, trial, and appeal), and not for any other purpose. Except when preparing a potential witness, the defense shall not show or make the discovery materials available by any means (electronic, physical or otherwise) to any person who is not a member of the defense, absent further order of this Court. Once a potential witness has also signed and agreed to be bound by the terms of this Protective Order, the defense may show the potential witness discovery materials necessary to prepare them, but may not give or allow the potential witness to retain the discovery materials or copies of them.

4. Each person receiving access to the discovery materials, including members of the defense, shall sign and date a copy of this Order to indicate their understanding of, acknowledgment of, and agreement to abide by its terms. No one may review the discovery materials unless he or she first signs a copy of this Order. Defense counsel shall keep the signed copies in the event of a disclosure or use of discovery materials prohibited by this Order.



Defense counsel shall not be required to disclose to the Government who has been given access to what discovery materials, absent further order of this Court following an opportunity to be heard.

5. Defense counsel shall promptly notify the Government and this Court if any discovery materials are disclosed either intentionally or unintentionally to anyone not designated by this Order or further order of the Court. Each member of the defense and potential witness provided access to discovery materials shall promptly notify defense counsel of any such disclosures.

6. At the end of these proceedings, including any potential appeals, the defense shall destroy all copies of discovery materials received and made by it. Defense counsel may keep one copy of all discovery materials for such additional time as they deem necessary to ensure their ability to satisfy all professional obligations to Defendant in this matter.

7. The Government shall make copies of the four hard drives delivered to the Government pursuant to an agreement between JSTOR and Defendant Swartz dated June 4, 2011, and "Downloaded Data" as defined in that agreement contained on a Maxtor hard drive seized by the government on January 6, 2011 available for review by the defense at the Boston Office of the Secret Service at mutually convenient times. During any review conducted by the defense, the Secret Service shall make an agent otherwise unaffiliated with the investigation and prosecution of this case available to provide assistance. This agent shall not communicate with the prosecution team about what items the defense reviews, except at the request of Defendant Swartz or with prior approval of the Court.

8. Nothing in this protective order is intended to otherwise restrict the proper use by

the defense of any discovery materials during the investigation, pre-trial litigation, trial preparation, trial or appeal of this matter.

SO ORDERED.

Date:

---

JUDITH G. DEIN  
United States Chief Magistrate Judge

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES	)	
OF AMERICA	)	
	)	
v.	)	Crim. No. 11-CR-10260-NMG
	)	
AARON SWARTZ,	)	
Defendant.	)	

**DEFENDANT'S MOTION TO COMPEL DISCOVERY**

Pursuant to Local Rule 116.3(G) and the September 9, 2011 order of this Court, Aaron Swartz moves this Court for an order compelling the government to provide discovery as provided by F.R. Crim. Proc. 16 and by the automatic discovery provisions in Rules 116.1(A)(1) and (C) and 116.2. The grounds for this motion are stated in the accompanying memorandum of law. A proposed order is attached to this motion as Exhibit A.

Respectfully submitted,

/s/Andrew Good  
Andrew Good  
BBO # 201240  
Good & Cormier  
83 Atlantic Avenue  
Boston, MA 02110  
Tel. 617-523-5933  
agood@goodcormier.com

**CERTIFICATE OF SERVICE**

I hereby certify that the foregoing document filed through the ECF system will be sent to counsel for the government who are registered participants as identified on the Notice of

Electronic Filing (“NEF”).

DATED: September 27, 2011

/s/ Andrew Good  
Andrew Good

G:\CLIENTS\Swartz, Aaron\Pleadings - Federal Court Case\Defendant's Motion to Compel Discovery dr1.doc

# **Exhibit A**

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Crim. No. 11-CR-10260-NMG
	)	
AARON SWARTZ,	)	
Defendant	)	

**(PROPOSED) ORDER**

After consideration of the Government's motion for a protective order, the Defendant's motion to compel discovery, and the oppositions filed by both parties in response to the motions, it is ordered that the Government shall provide copies, or enable the Defendant to make copies, of the following that are within its possession, custody or control:

1. All electronic data that constitutes or includes a written statement of Mr. Swartz including communications on Twitter, Facebook, text message and email or any other form of electronic communication.
2. All data, documents, and tangible things including, but not limited to, data obtained from MIT and JSTOR, that are discoverable under Rule 16(a)(1)(E).

All data includes: (A) all data seized from devices that the government has asserted belong to the defendant, including:

- Acer laptop computer recovered at MIT
- Western Digital hard drive recovered at MIT\*
- HP USB drive seized from the defendant at the time of his arrest
- Apple iMac computer seized at Harvard
- Western Digital hard drive seized at Harvard
- HTC G2 cell phone seized during the search of the defendant's residence

---

\* Search warrant applications for devices seized at MIT and Harvard allege probable cause to believe that these devices belong to Mr. Swartz and are evidence of the commission of the offenses charged in the indictment.

- Nokia 2320 cell phone seized during the search of the defendant's residence
- Sony Micro Vault seized during the search of the defendant's residence

(B) All data and items that are material to preparing the defense, namely, all data and items that constitute, or are evidence of, the occurrences and activity, including electronic communications, transmissions, and activity, that the government alleges occurred in the indictment.

(C) All data and items that the government intends to use in its case-in-chief.

3. All data, documents, and tangible things that constitute or are evidence of the potentially exculpatory information described in paragraph H.1 and H.5 of the government's August 12, 2011 letter to defense counsel other than the fingerprint data that has already been produced.
4. Full and complete copies of all video recordings made inside the wiring closet in the basement of MIT Building 16 including, but not limited to, recordings made on January 4 and 6, 2011.
5. All data, documents, and tangible things that constitute or are evidence of the eyewitness identification procedure mentioned in paragraph G of the government's August 12, 2011 letter to defense counsel.

When the data referred to in this order is computerized electronic data, transmissions, or communications, the government shall provide copies, or enable the defense to make copies, of the data in its native, bit-by-bit form, including all metadata, if the government has the data in its native format including all metadata. If the government does not have the data in its native form, including all metadata, it is to provide copies or enable the defense to make copies in the same computer searchable format of the data



that is within in the possession, custody and control of the government, including optical character recognition software format.

SO ORDERED.

Date:

---

JUDITH G. DEIN  
United States Chief Magistrate Judge

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES	)	
OF AMERICA	)	
	)	
v.	)	Crim. No. 11-CR-10260-NMG
	)	
AARON SWARTZ,	)	
Defendant.	)	

**DEFENDANT’S MEMORANDUM OF LAW  
IN SUPPORT OF HIS MOTION TO COMPEL DISCOVERY**

Pursuant to Local Rule 116.3(G) and the September 9, 2011 order of this Court, Aaron Swartz moves this Court for an order compelling the government to provide discovery as provided by F.R. Crim. Proc. 16 and by the automatic discovery provisions in Rules 116.1(A)(1) and (C) and 116.2. The government has not provided a very substantial portion of the information and documents required to be disclosed by these rules. Instead, it has withheld automatically discoverable information and documents, and demanded that the defense agree to an unjustified protective order as a pre-condition to receipt of discovery. Without good cause, the government has withheld the following:

- 1. Defendant’s Written Statements.** The defendant’s written statements that are within its custody, possession and control, e.g., Twitter and Facebook postings, websites, text messages and electronic mail. The government obtained some of this information as the fruit of warrantless seizures of devices that the government asserts belong to Mr. Swartz; some are the fruit of warrant-authorized seizures of items that the government asserts belong to Mr. Swartz; and, some information was obtained in response to grand jury subpoenas to electronic communications providers. The defendant’s written statements are subject to automatic discovery.

Local Rule 116.1(C)(1)(a) and Rule 16(a)(E). In paragraph A.1.a. of its August 12, 2011 letter to defense counsel (attached hereto as Exhibit 1), the government states that it will offer some of these written statements in its case-in-chief. The defendant's written statements are also material to the defense. The government does not provide any "good cause" for withholding the defendant's written statements.

**2. Seized Electronic Data.** In its August 12, 2011 letter, the government listed the items containing electronic data stored in electronic data storage media that it has seized as follows:

- Acer laptop computer recovered at MIT
- Western Digital hard drive recovered at MIT\*
- HP USB drive seized from the defendant at the time of his arrest
- Apple iMac computer seized at Harvard
- Western Digital hard drive seized at Harvard
- HTC G2 cell phone seized during the search of the defendant's residence
- Nokia 2320 cell phone seized during the search of the defendant's residence
- Sony Micro Vault seized during the search of the defendant's residence

The government has no good cause to withhold copies of the seized electronic data, all of which is discoverable under Rule 16(a)(1)(E). For that reason, the instant motion seeks an order compelling the government to provide the defense with copies in the form of bit-by-bit, mirror electronic images of all of the data natively stored on the above-listed electronic devices, including any and all metadata. In order to effectively defend against the indictment's allegations, Mr. Swartz is constitutionally entitled to an exact and complete copy of the discoverable electronically stored information in its native format so that he may

---

\* Search warrant applications for devices seized at MIT and Harvard allege probable cause to believe that these devices belong to Mr. Swartz and are evidence of the commission of the offenses charged in the indictment.

examine and, if appropriate, contest the provenance and substance of that evidence. *See United States v. Briggs*, 2011 U.S. Dist. LEXIS 101415 (W.D.N.Y.).

- 3. Electronic Data Obtained From Non-Parties.** The government's August 12, 2011 letter states all documents and tangible objects that are material to the defense including, but not limited to, items obtained from MIT and JSTOR are being withheld. In its letter, the government asserts that:

Because many of these items contain **potentially sensitive, confidential, and proprietary communications, documents and records** obtained from MIT and JSTOR, including discussions of victims' computer systems and security measures, we will need to arrange a protective order with you before inspection.

Exhibit 1 at 2 (emphasis added). Rule 16(d)(1) authorizes this Court to enter protective orders concerning information provided in discovery. However, the movant for such a protective order must make a showing of "good cause" for the entry of such an order.

The First Circuit has not provided guidance to the lower courts concerning the factors to be taken into account in determining whether a movant has shown Rule 16(d)(1) "good cause," except in cases involving disclosure of classified national security secrets under the Classified Information Procedure Act (CIPA). *United States v. Pringle*, 751 F.2d 419, 427-428 (1<sup>st</sup> Cir. 1984). Certainly, the information being withheld is not classified as secret for national security reasons. There is no allegation that the withheld information concerns an endangered confidential informant, or that there is any evidence to support a concern about witness intimidation or safety. *United States v. Barbeito*, 2009 U.S. Dist. LEXIS 102688 (S.D. W.Va. 2009). The third-party-sourced documents are not child

pornography or any other contraband. The government has no basis to claim that the withheld information is privileged (*United States v. Thompson*, 562 F.3d 387 (D.C. Cir. 2009)(work product privilege), patented (stipulated protective order in *United States v. Pani*, 08-CR 40034-FDS), or copyrighted. Unlike, the agreed order entered in *United States v. Gonzalez*, 2009 U.S. Dist. LEXIS 50791 (D.Mass. 2009), there is no personal financial information involved here, such as the credit card or social security numbers of consumers.

The government's unsupported assertion that some part of the third-party-sourced information may be "**potentially sensitive, confidential, and proprietary**" falls far short of good cause. The government asserts that some of the information includes discussion of the computer systems of MIT and JSTOR and security measures. This information is discoverable because it constitutes putative evidence that will be publicly disclosed in this litigation, including a public trial. The Court's September 9, 2011 order allows Mr. Swartz to oppose the government's motion for a protective order but, certainly, nothing in the government's August 12, 2001 letter to defense counsel constitutes good cause to impose a protective order concerning any third-party-sourced information.

- 4. Electronically-Stored Information Provided by the Defendant.** The government is withholding and refusing to provide a copy of the electronic data stored in four Samsung hard drives delivered to the Secret Service by Mr. Swartz on June 7, 2011, at the office of undersigned counsel. The government has made no showing of good cause concerning this data which it would not have in its custody and control, but for Mr. Swartz's delivery of it to the government.

- 5. Complete Video Recordings.** Paragraph E of the government's August 12, 2011 letter states that it has provided copies of what it considers to be the "relevant portions" of video recordings made on January 4 and 6, 2011, in a wiring closet in the basement of MIT's Building 16. Under Rule 16, Mr. Swartz is entitled to full and complete copies of all video recordings made in that closet including but not limited to recordings made at any time including, but not limited to, January 4 and 6, 2011, because the complete records contain evidence that is material to his defense.
- 6. Identifications.** Paragraph G of the government's letter provides documents related to an identification procedure involving the use of a photo array but redacts all identifying information concerning the alleged eyewitness on the unfounded ground that the eyewitness has a right of privacy at this stage of the litigation. Rule 16 does not authorize redaction of information from discoverable documents. The purpose of this discovery rule is to enable the defense to move early in the proceeding to suppress eyewitness testimony, if the eyewitness was subjected to suggestive statements or activity by investigating officials. The purpose of the rule is undermined and rendered ineffective if the identity of the alleged eyewitness is withheld, because no effective investigation of the identification can be conducted without identifying information about the alleged eyewitness. Nothing in the government's letter provides any basis for defeating the purpose of the rule.
- 7. Exculpatory Evidence.** In paragraph H of the government's letter, the government described but refused to provide almost all of certain exculpatory

evidence, including evidence that, during the period covered by the indictment, persons other than Mr. Swartz at Harvard, MIT and China accessed the Acer laptop that was seized by the government, and persons other than Mr. Swartz at MIT and elsewhere were engaging in “journal spidering” of JSTOR data using a “virtual computer” that can be hosted by anyone at MIT. The government has no basis for withholding the electronic evidence described as exculpatory in its letter.

The government’s letter at page 6 discloses that one of its witnesses has publicly-filed criminal charges pending against him or her, but withholds the name of the witness, purportedly on privacy grounds. The government has not disclosed the documents that mention the publicly-filed criminal charge against the witness. It is obliged by rule and by constitutional principles to disclose those documents. There is no legal basis for redacting the documents or withholding the identity of the witness. The purpose of the automatic discovery rule requiring early disclosure of exculpatory evidence is undermined by withholding witness identifying information.

**Conclusion.** Because the government has no valid basis for having withheld the discoverable information and evidence itemized in this memorandum, Mr. Swartz urges this Court to issue an order compelling the government to provide, or enable the defense to make, bit-by-bit, mirror image copies of native electronic data that constitute the written statements of the defendant, evidence seized by the government as listed in the motion, third-party-sourced evidence including, but not limited to, evidence from MIT and JSTOR, evidence provided to the government by Mr. Swartz, and exculpatory evidence. The order should also compel the government to disclose the complete video



recordings, and identifying information concerning the alleged eyewitness who was exposed to the photo array and the witness who has publicly-filed criminal charges pending against him or her, as well as all documents that mention those criminal charges.

Respectfully submitted,

/s/Andrew Good  
Andrew Good  
BBO # 201240  
Good & Cormier  
83 Atlantic Avenue  
Boston, MA 02110  
Tel. 617-523-5933  
agood@goodcormier.com

CERTIFICATE OF SERVICE

I hereby certify that the foregoing document filed through the ECF system will be sent to counsel for the government who are registered participants as identified on the Notice of Electronic Filing ("NEF").

DATED: September 27, 2011

/s/ Andrew Good  
Andrew Good

G:\CLIENTS\Swartz, Aaron\Pleadings - Federal Court Case\Defendant's Motion to Compel Discovery dr2.doc

# **Exhibit 1**



**U.S. Department of Justice**

***Carmen M. Ortiz***  
*United States Attorney*  
*District of Massachusetts*

---

*Main Reception: (617) 748-3100*

*United States Courthouse, Suite 9200*  
*1 Courthouse Way*  
*Boston, Massachusetts 02210*

August 12, 2011

Mr. Andrew Good  
Good and Cormier  
83 Atlantic Avenue  
Boston, MA 02110

Re: United States v. Aaron Swartz  
Criminal No. 11-CR-10260

Dear Counsel:

Pursuant to Fed. R. Crim. P. 16 and Rules 116.1(C) and 116.2 of the Local Rules of the United States District Court for the District of Massachusetts, the government provides the following automatic discovery in the above-referenced case:

A. Rule 16 Materials

1. Statements of Defendant under Rule 16 (a)(1)(A) & (a)(1)(B)

a. Written Statements

The defendant's booking sheet and fingerprint card from the Cambridge Police Department are contained on enclosed Disk 5.

There are numerous relevant statements not made to government agents drafted by Defendant Swartz before the date of his arrest contained in electronic media, such as Twitter postings, websites and e-mail. These are equally available to the defendant. Those that the government intends to use in its case-in-chief are available for your review, as described in paragraph A(3) below.

Subject thereto, there are no relevant written statements of Defendant Swartz made

following his arrest in the possession, custody or control of the government, which are known to the attorney for the government.

b. Recorded Statements

The defendant made recorded statements at the time of his booking by Cambridge Police on January 6, 2011. A copy of his booking video is enclosed on Disk 7.

c. Grand Jury Testimony of the Defendant

Defendant Aaron Swartz did not testify before a grand jury in relation to this case.

d. Oral Statements to Then Known Government Agents

Defendant Aaron Swartz made oral statements at the time of the search of his apartment to individuals known to him at the time to be government agents. The only statements made by him then which the government believes at this time to be material are memorialized in the affidavit in support of the search warrant for his office at Harvard, a copy of which affidavit is enclosed on Disk 3.

2. Defendant's Prior Record under Rule 16 (a)(1)(D)

Enclosed on Disk 3 is a copy of the defendant's prior criminal record.

3. Documents and Tangible Objects under Rule 16(a)(1)(E)

All books, papers, documents and tangible items which are within the possession, custody or control of the government, and which are material to the preparation of the defendant's defense or are intended for use by the government as evidence in chief at the trial of this case, or were obtained from or belong to the defendant, may be inspected subject to a protective order by contacting the undersigned Assistant U.S. Attorney and making an appointment to view the same at a mutually convenient time.

Because many of these items contain potentially sensitive, confidential and proprietary communications, documents, and records obtained from JSTOR and MIT, including discussion of the victims' computer systems and security measures, we will need to arrange a protective order with you before inspection. Please review the enclosed draft agreement and let us know your thoughts.

4. Reports of Examinations and Tests under Rule 16 (a)(1)(F)

Enclosed you will find Disks 1, 2, 5 & 6 containing reports of examination of the following:

- Acer laptop computer recovered at MIT
- Western Digital hard drive recovered at MIT
- HP USB drive seized from the defendant at the time of his arrest
- Apple iMac computer seized at Harvard
- Western Digital hard drive seized at Harvard
- HTC G2 cell phone seized during the search of the defendant's residence
- Nokia 2320 cell phone seized during the search of the defendant's residence
- Sony Micro Vault seized during the search of the defendant's residence
- Four Samsung hard drives delivered to the Secret Service by Defendant Swartz and his counsel on June 7, 2011 (Please note that because of the number of files contained on Samsung model HD154UI hard drive, serial number S1Y6J1C2800332, it has not been practicable to date to make a complete file list in an Excel readable format, unlike the other drives.)
- A fingerprint analysis report from the Cambridge Police Department with respect to the Acer Laptop and Western Digital hard drive recovered at MIT
- A supplemental fingerprint analysis report with respect to these items

While not required by the rules, intermediate as well as final forensic reports where available are enclosed for many of the recovered and seized pieces of equipment on Disks 6 and 1, respectively.

B. Search Materials under Local Rule 116.1(C)(1)(b)

Search warrants were executed on multiple pieces of electronic equipment and at multiple locations. Copies of the search warrants, applications, affidavits, and returns have already been provided to you, but are further found on Disk 3.

Four Samsung Model HD154UI hard drives were examined following their consensual and unconditional delivery to the United States Secret Service on June 7, 2011. As an additional precaution, a warrant, enclosed on Disk 3, was also obtained.

C. Electronic Surveillance under Local Rule 116.1(C)(1)(c)

No oral, wire, or electronic communications of the defendant as defined in 18 U.S.C. § 2510 were intercepted relating to the charges in the indictment.

D. Consensual Interceptions under Local Rule 116.1(C)(1)(d)

There were no interceptions (as the term "intercept" is defined in 18 U.S.C. § 2510(4)) of wire, oral, or electronic communications relating to the charges contained in the indictment, made with the consent of one of the parties to the communication in which the defendant was intercepted or which the government intends to offer as evidence in its case-in-chief.

E. Video Recordings

On January 4, 2011 and January 6, 2011, Defendant Aaron Swartz was recorded entering a restricted wiring closet in the basement of MIT's Building 16. Copies of relevant portions of the recordings (where he is seen entering, in, or exiting the closet) are enclosed on Disk 4.

F. Unindicted Coconspirators under Local Rule 116.1(C)(1)(e)

There is no conspiracy count charged in the indictment.

G. Identifications under Local Rule 116.1(C)(1)(f)

Defendant Aaron Swartz was a subject of an investigative identification procedure used with a witness the government anticipates calling in its case-in-chief involving a photospread documented by MIT Police Detective Boulter. Relevant portions of the police report of Detective Boulter and a copy of the photospread used in the identification procedure are enclosed on Disk 3. In both instances, the name of the identifying MIT student has been redacted to protect the student's continuing right to privacy at this initial stage of the case. On page 2 of the Report of Photo Array, USAO-000007, the initials beside each of the enumerated items have been redacted for the same reason.

H. Exculpatory Evidence Under Local Rule 116.2(B)(1)

With respect to the government's obligation under Local Rule 116.2(B)(1) to produce "exculpatory evidence" as that term is defined in Local Rule 116.2(A), the government states as follows:

1. The government is unaware of any information that would tend directly to negate the defendant's guilt concerning any count in the indictment. However, the United States is aware of the following information that you may consider to be discoverable under Local Rule 116.2(B)(1)(a):
  - Email exchanges between and among individuals at MIT and JSTOR as they sought to identify the individual responsible for massive downloads on the dates charged in the Indictment. While the defendant has admitted to being responsible for the downloads and produced one copy of most of what was downloaded on these dates, these e-mails reflect JSTOR's and MIT's initial difficulties in locating and identifying him in light of the furtive tactics he was employing. The email exchanges will be made available in accordance with paragraph (A)(3) above.
  - Counsel for the government understands that a number of external connections were made and/or attempted to the Acer laptop between January 4, 2011 and January 6, 2011, including from a Linux server at MIT and from China. The Linux server was connected to a medical center at Harvard periodically during the same period. While government

counsel is unaware of any evidence that files from JSTOR were extracted by third parties through any of these connections, the connection logs will be made available to you in accordance with paragraph (A)(3) above.

- An analysis of one of the fingerprints on the Acer laptop purchased and used by the defendant cannot exclude his friend, Alec Resnick. The analysis is being produced for you; see paragraph (A)(4) above.
- While not a defense or material, one or more other people used or attempted to use scrapers to download JSTOR articles through MIT computers during the period of Defendant Swartz's illegal conduct. On the evening of November 29, 2010, the network security team at MIT was contacted and investigated journal spidering occurring on the site of the Institute of Electrical and Electronic Engineers. It was tracked to a group of shared computers on which anyone at MIT can host a virtual machine. It was determined that a virtual machine had been compromised. The user was notified that scripts placed on it were downloading journals from JSTOR, IEEE and APS. The machines were taken offline early the morning of November 30, 2010.
- The login screen on the Acer laptop when observed by Secret Service Agent Pickett on January 4, 2011 identified the user currently logged in as "Gene Host." A user name is different from a host name, and accordingly is similarly immaterial.

2. The government is unaware of any information that would cast doubt on the admissibility of evidence that the government anticipates offering in its case-in-chief and that could be subject to a motion to suppress or exclude.

3. Promises, rewards, or inducements have been given to witness Erin Quinn Norton. Copies of the letter agreement with her and order of immunity with respect to her grand jury testimony are enclosed on Disk 3.

4. The government is aware of one case-in-chief witness who has a criminal record.

Please be advised that one of the government's prospective trial witnesses was the subject of a charge in Somerville District Court in 1998 of being a minor in possession of alcohol and that the case was dismissed the following month upon payment of court costs. The government intends to make no further disclosures with respect to this matter, as the criminal charge could have no possible admissibility under either Fed.R.Crim.P. 609 or 608(b). If you believe you are entitled to additional information, including the identity of the prospective witness, please advise the undersigned, in which event the government will seek a protective order from the court to permit non-disclosure.

5. The government is aware of one case-in-chief witnesses who has a criminal case pending.

Please be advised that one of the government's prospective trial witnesses has pending state charges brought on July 7, 2009, involving the Abuse Prevention Act, Possession of Burglarious Tools, Criminal Harassment, and Breaking and Entering in the Daytime With Intent to Commit a felony. The events underlying the charges arise from the break-up of a personal relationship. The government has withheld the name of the witness and the others involved to protect their privacy, but will make them available along with the police reports in its possession subject to a protective order ensuring that the names, events and reports will not be disclosed publicly until the trial of this case, should the Court determine that a charge or information contained in the police reports is admissible for the purposes of cross-examination.

6. Based on the timeline as the government presently understands it from Officer Boulter's report described in paragraph G above and contained on Disk 3, no named percipient witnesses failed to make a positive identification of the defendant with respect to the crimes at issue. As reflected in the report, three students present when the Acer computer and Western Digital hard drive were recovered from Building 20 by law enforcement stated that they did not see anyone come in and place the computer there. However, as the timeline reflects, this was not a failed identification, but rather that they were not percipient witnesses to the event which had occurred earlier.

#### I. Other Matters

The government has preliminary analysis notes prepared at Carnegie Mellon of certain code and files contained on the Acer Laptop, as referenced on Page 2 of SA Michael Pickett's Forensic Cover Report contained on Disk 1. While these are not encompassed by Rule 16 (a)(1)(F) (formerly 16(a)(1)(D)), the government will make these available for review as described in section (A)(3), above, subject to the same procedures proscribed for preliminary transcripts in Local Rule 116.4 (B)(2).

Your involvement in the delivery of four hard drives containing documents, records and data obtained from JSTOR creates potential issues in this case under the Rules of Professional Conduct, as I am sure you are aware. To avoid the potential for those issues under Rule 3.7 in particular, we propose a stipulation from your client that the hard drives were from him, thus taking you out of the middle and rendering the origin an uncontested issue under the Rule. This stipulation would be without prejudice to all arguments on both sides as to the admissibility of the drives and their contents at any proceeding.

The government is aware of its continuing duty to disclose newly discovered additional evidence or material that is subject to discovery or inspection under Local Rules 116.1 and 116.2(B)(1) and Rule 16 of the Federal Rules of Criminal Procedure.

The government requests reciprocal discovery pursuant to Rule 16(b) of the Federal Rules of Criminal Procedure and Local Rule 116.1(D).



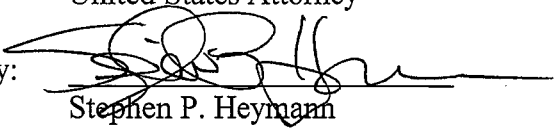
The government demands, pursuant to Rule 12.1 of the Federal Rules of Criminal Procedure, written notice of the defendant's intention to offer a defense of alibi. The time, date, and place at which the alleged offenses were committed is set forth in the indictment in this case a copy of which you previously have received.

Please call the undersigned Assistant U.S. Attorney at 617-748-3100 if you have any questions.

Very truly yours,

CARMEN M. ORTIZ  
United States Attorney

By:



Stephen P. Heymann  
Scott L. Garland  
Assistant U.S. Attorneys

enclosures

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES	)	
OF AMERICA	)	
	)	
v.	)	Crim. No. 11-CR-10260-NMG
	)	
AARON SWARTZ,	)	
Defendant.	)	

**DEFENDANT’S OPPOSITION TO  
MOTION OF THE UNITED STATES FOR A PROTECTIVE ORDER**

Defendant, Aaron Swartz, submits this opposition to the Government’s motion for a protective order, including the proposed order attached thereto. Dkt. No. 18. Mr. Swartz has filed a cross-motion to compel with a proposed order attached thereto as Exhibit A. Dkt. No. 19. He has also filed a memorandum of law. Dkt. No. 20.

At the outset, it is critical to note that the Government acknowledges that all of the documents and information it has withheld are automatically discoverable under this Court’s local rules or Rule 16, or both. It does not argue that these rules do not require disclosure of the withheld documents and information. It does not argue that there is any reason to delay these disclosures either. The Government’s motion provides no lawful basis for the entry of its proposed protective order.

**I. THE INDICTMENT’S UNPROVEN ALLEGATIONS CANNOT  
ESTABLISH “GOOD CAUSE” FOR THE ISSUANCE OF THE  
GOVERNMENT’S PROPOSED ORDER.**

Both the first paragraph of the Government’s proposed order and its motion rely on the indictment’s unproven allegations, as if this Court may rely on them as evidence to support a finding of good cause to enter a protective order under Rule 16(d)(1). The government would have this Court find that JSTOR and MIT are “victims” before the

trial. The Government cites no legal authority for any of this, because there is none. The Government is urging this Court to obliterate the presumption of innocence and the Government's burden of proof at trial. It would have this Court call this abrogation of Mr. Swartz's constitutional rights "good cause." The Government says that some of its evidence "cannot be disputed," but its position urges the Court to accept the Government's representations as fact, its version of the evidence and its supposed indisputable nature as truth or, at a minimum, to presume that the Government's representations are true. All of that is prohibited the Constitution.

Based on this unconstitutional predicate, the Government urges this Court to find that Mr. Swartz presents a "very real risk of serious and irreparable harm." Gov. Motion at 1. There is nothing in the record that can support such an unconstitutional finding. Indeed, the evidence pertaining to Mr. Swartz's trustworthiness includes the following: (1) Mr. Swartz appeared voluntarily for arraignment; (2) Mr. Swartz has been in full compliance with the conditions of his release; (3) on June 7, 2011, months prior to his arraignment, Mr. Swartz provided certain hard drives to the Government. The Government's August 12, 2011 letter states that this was a "consensual and unconditional delivery." There is absolutely no basis in this record to find that Mr. Swartz cannot be trusted to use the discovery and assist in the presentation of his defense in a lawful manner.

**II. THE GOVERNMENT'S UNSUPPORTED AND UNPROVEN ALLEGATIONS CANNOT SUPPORT A FINDING THAT THE WITHHELD DOCUMENTS AND INFORMATION ARE "SENSITIVE, CONFIDENTIAL OR PROPRIETARY."**

**A. The Categories of Withheld Documents and Information Are Overbroad and Completely Unjustified.**

The Government has withheld the following: (1) the defendant's written statements, including statements that it intends to offer in its case-in-chief; (2) software that it alleges Mr. Swartz wrote and used to commit the offenses alleged in the indictment; and (3) evidence seized from Mr. Swartz's residence and workplace including:

- Acer laptop computer recovered at MIT
- Western Digital hard drive recovered at MIT\*
- HP USB drive seized from the defendant at the time of his arrest
- Apple iMac computer seized at Harvard
- Western Digital hard drive seized at Harvard
- HTC G2 cell phone seized during the search of the defendant's residence
- Nokia 2320 cell phone seized during the search of the defendant's residence
- Sony Micro Vault seized during the search of the defendant's residence

The Government has overbroadly, and without any justification, withheld documents and information that it alleges was written by, or sourced from, Mr. Swartz, even though it has not shown that any of this information is sensitive, confidential, proprietary or valuable.

For example, the Government argues speciously that Mr. Swartz's access should be restricted to software code even though it alleges that Mr. Swartz authored and used that very software code. If its allegation is correct, Mr. Swartz has always been fully capable of writing the code again now, and broadcasting it if he so chooses. He has not done so. The Government provides no basis whatsoever for withholding or restricting Mr. Swartz's access to his own written statements and the evidence it seized from computers that it alleges belonged to Mr. Swartz. The fact that this information has been withheld unjustifiably makes it clear that the

---

\* Search warrant applications for devices seized at MIT and Harvard allege probable cause to believe that these devices belong to Mr. Swartz and are evidence of the commission of the offenses charged in the indictment.

Government is seeking to burden Mr. Swartz in the conduct of his defense for no legitimate reason.

**B. The Withheld Documents Are Not Sensitive, Confidential, Proprietary or Valuable.**

Under the rules of civil and criminal procedure, litigants in this Court are not permitted to withhold documents from discovery, or to claim entitlement to protective orders, simply because they make self-serving and unsubstantiated claims that the documents or information are not discoverable on the same terms as any other discoverable materials. The Government is not exempt from having to substantiate its claims with evidence, nor is any proffered substantiation immune from adversarial challenge. This is particularly true when discovery provided for by the Rules of Criminal Procedures is an essential assurance of the fairness of criminal trials, and the accuracy of verdicts that can deprive a person of his or her liberty.

The Government's bare assertion that the withheld documents and information are "potentially sensitive, confidential, and proprietary" (Gov. Order at 1, emphasis supplied) or "very valuable" (Gov. Motion at 2) falls far short of providing any evidentiary and lawful basis for the issuance of a protective order. The Government cannot and does not say that any of the withheld information is actually "sensitive" (a term that has no legal meaning in this criminal discovery context), confidential, or proprietary. Tellingly, the Government claims only that the withheld information is "potentially" sensitive, confidential, and proprietary. The Government has provided zero evidence to support a judicial finding that any of the withheld documents and information, much less all of that material, is actually "sensitive, confidential, and proprietary" or "very valuable."

**C. The Government's Purported Justifications For Withholding Discoverable Documents and Information Are Unsupported by Evidence and Any Such Evidence Must Be Subject to Adversarial Challenge.**

This Court lacks authority to approve the Government's proposal to impose the significant and unwarranted burdens on Mr. Swartz's ability to participate efficiently and effectively in his own defense, without the Government presenting evidence that can be subjected to adversarial scrutiny and challenge. In a footnote to its motion, the Government says, "A JSTOR representative will address this issue before the Court at hearing on this motion." Dkt. No. 18 at 3 n.1. This cannot be permitted. If the Government has evidence to support the purported justifications for imposing a burden on Mr. Swartz's participation in his defense, it must be presented in evidentiary form so that it can be subjected to cross-examination and adversarial challenge. When litigants assert rights to withhold discovery or seek to impose restrictions on access, they must do so under oath in evidentiary form. Such claims are then properly subject to adversarial challenge. The government has had months to present such evidence, and it has failed to do so.

**III. THE RESTRICTIONS PROPOSED BY THE GOVERNMENT ARE UNJUSTIFIED AND IMPROPERLY INTERFERE WITH THE EFFECTIVE AND EFFICIENT FUNCTIONING OF THE DEFENSE.**

**A. Restrictions on Documents Other Than Data on External Drives Delivered by Mr. Swartz.**

In substance, paragraphs 2 and 3 of the Government's proposed order prohibit Mr. Swartz from having copies of documents and information provided by the Government. Under the Government's proposal, the documents cannot be electronically transmitted to Mr. Swartz by his counsel, investigators or experts.

Paragraph 3 prohibits the defense from displaying the documents and information to prospective trial witnesses unless they first sign the protective order. These restrictions impose burdens on the cost-efficient and effective functioning of the defense. The Court cannot impose handicaps on the defense's functioning without substantial evidence justifying them. No such evidence has been proffered.

The most important member of the defense team is Mr. Swartz. This case centers on complex issues concerning the operation for several months of complex computers and computer networks, software written in computer languages, etc. Mr. Swartz works during the day, mostly in New York City. Undersigned counsel works in Boston during the day. The defenses experts are not in New York or Boston and work during the day. His investigators are not in New York. Mr. Swartz must work on his case during nights and weekends. His work will consume a great many hours. It is prohibitively expensive to require Mr. Swartz to have to work with the discovery materials in the presence of a court-ordered supervisor. The gain from having Mr. Swartz work in the presence of others is non-existent. He must be able to take notes and write memos for the defense team based on what he examines. He can recall what he examines. The supposed gain in data security sought by the Government is slight to non-existent, but the expensive handicap imposed on the defense is prohibitive.

The prohibition of transmission of the materials to and from Mr. Swartz makes it impossible to conduct timely, effective and efficient, interactive consultation between Mr. Swartz and his defense team. It is absolutely essential for Mr. Swartz and the defense team to be able to circulate, annotate and comment on the details in the

discoverable documents without Mr. Swartz having to be in the presence of anyone when he works on this case. That kind of free and frequent communication at all hours is essential to the functioning of the defense including, but not limited to, the period shortly before and during the trial.

The Government will not be similarly restricted. It can freely provide whatever information it wants, by whatever means, to the prosecution team and potential witnesses. The Rules of Criminal Procedure are designed to preserve – not skew – the balance of litigation advantage in the exchange and use of discoverable information. Nothing in the record supports a finding that Mr. Swartz will obstruct justice or abuse discoverable information. To the contrary, all of the evidence supports Mr. Swartz's trustworthiness as a litigant who is presumed innocent in this case.

**B. Restrictions Pertaining to Data Delivered to the Government by Mr. Swartz.**

The government claims that only the government has the ability to secure the data on the drives Mr. Swartz delivered to the government from being obtained by third parties. Without the slightest evidence to support its assertion, the Government would have this Court rule as if the defense's facilities lack adequate security for this purpose. Undersigned counsel has secured from intrusion and theft highly confidential information for decades without a single security breach. There is absolutely no reason to doubt that the defense cannot store and use the information securely. But, in reality, the Government's proposed order imposes prohibitive, logistical and security problems for the defense.

**First**, any defense examination of the data delivered by Mr. Swartz to the



Government entails making an electronic record in that data of the defense's searches and examination of the data. The defense may need to install and use its own software to conduct its examination on a government-controlled computer. The defense will need to make copies of certain information for purposes of investigation, trial preparation and trial. If the government's proposed order is approved, all of that information must be included in data that remains in the custody of the Government. All of this is unquestionably work product information. Paragraph 4 of the Government's proposed order would require the defense's work product privileged information to be in the custody of the Government. This chills the defense's activities. This cannot be reconciled with the Sixth Amendment right to counsel. The government's work product will not be similarly exposed. The lack of even handedness violates due process fairness. There is no legal authority to impose such unconstitutional burdens on the defense.

**Second**, the proposed protective order would require the defense to work on a Government-controlled schedule and in a Government-selected location on Government-controlled computers. There is absolutely no justification for hobbling the defense in this manner. The defense must be agile and absolutely independent. It should not be dependent on having to make arrangements with the Government to work at times and under conditions that the government deems feasible.

**Third**, much of the supposedly proprietary and valuable information allegedly on the drives delivered by Mr. Swartz is in the public domain either due to JSTOR's actions or other reasons. For example, on September 6, 2011, weeks after this indictment was returned, JSTOR's website made what it terms "Early Journal

Content” consisting of “nearly 500,000 articles” publicly accessible to anyone.

JSTOR also stated its intention to make additional releases of articles. See JSTOR announcement attached hereto as Exhibit 1. In practical terms, the Government is urging this Court to require the defense to examine in a Government office approximately 500,000 articles that are publicly accessible for free or have been made publicly accessible for free by JSTOR. All of the articles in JSTOR’s database can be freely accessed in libraries.

Paragraph 4 of the proposed order applies to defense examination of huge amounts of non-proprietary, public domain information. For that reason, paragraph 4 is nonsensical and imposes an onerous and prohibitive burden on the defense for no legitimate reason.

## **VI. CONCLUSION**

For all the foregoing reasons, Mr. Swartz urges the Court to deny the Government’s motion for a protective order.

Respectfully submitted,

/s/Andrew Good  
Andrew Good  
BBO # 201240  
Good & Cormier  
83 Atlantic Avenue  
Boston, MA 02110  
Tel. 617-523-5933  
agood@goodcormier.com

CERTIFICATE OF SERVICE

I hereby certify that the foregoing document filed through the ECF system will be sent to counsel for the Government who are registered participants as identified on the Notice of Electronic Filing (“NEF”).

DATED: October 6, 2011

/s/ Andrew Good  
Andrew Good

# **Exhibit 1**



## EARLY JOURNAL CONTENT

149 Fifth Avenue, 8th Floor, New York, NY 10010 | tel (212) 358 6400 | fax (212) 358 6499 | participation@jstor.org | jstor.org

# Nearly 500,000 articles in more than 200 journals are now freely available on JSTOR.

Anyone may now search, read online, and download PDFs of “Early Journal Content.” The Early Journal Content includes journal articles published in the United States before 1923 and articles published in other countries before 1870, and includes discourse and scholarship in the arts and humanities, economics and politics, and in mathematics and other sciences.

The free Early Journal Content is available for use by anyone, without registration and regardless of institutional affiliation. The amount of free content will grow over time. As we add more journals to JSTOR, new articles within these time ranges will be added to the Early Journal Content, and will remain freely available.

Making this early journal content freely available is the most recent step in our ongoing work to expand access to content on JSTOR, particularly for individuals who are not affiliated with academic institutions or libraries. More efforts are planned for the future; currently in progress is a project to enable individual researchers to register with the JSTOR site to read more recent articles online for free.

## Access for Individuals

- [about.jstor.org/individuals](http://about.jstor.org/individuals)

## Early Journal Content

- [about.jstor.org/participate-jstor/individuals/early-journal-content](http://about.jstor.org/participate-jstor/individuals/early-journal-content)

## Terms and Conditions of Use

- [jstor.org/page/info/about/policies/terms.jsp](http://jstor.org/page/info/about/policies/terms.jsp)

### Early Journal Content Highlights

#### Democracy in Education

John Dewey  
The Elementary School Teacher  
Vol. 4, No. 4 (Dec., 1903), pp. 193–204  
Published by: The University of Chicago Press  
Article Stable URL: [jstor.org/stable/992653](http://jstor.org/stable/992653)

#### “General Intelligence,” Objectively Determined and Measured

C. Spearman  
The American Journal of Psychology  
Vol. 15, No. 2 (Apr., 1904), pp. 201–292  
Published by: University of Illinois Press  
Article Stable URL: [jstor.org/stable/1412107](http://jstor.org/stable/1412107)

#### Japanese Textiles at the Columbian Exposition

The Decorator and Furnisher  
Vol. 23, No. 2 (Nov., 1893), pp. 57–59  
Article Stable URL: [jstor.org/stable/25582570](http://jstor.org/stable/25582570)

#### Woman’s Half-Century of Evolution

Susan B. Anthony  
The North American Review  
Vol. 175, No. 553 (Dec., 1902), pp. 800–810  
Published by: University of Northern Iowa  
Article Stable URL: [jstor.org/stable/25150960](http://jstor.org/stable/25150960)

#### On the True Date of the Rosetta Stone, and on the Inferences Deducible from It

Edward Hincks  
The Transactions of the Royal Irish Academy  
Vol. 19, (1843), pp. 72–77  
Published by: Royal Irish Academy  
Article Stable URL: [jstor.org/stable/30079145](http://jstor.org/stable/30079145)

**UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS**

<b>UNITED STATES OF AMERICA</b>	)	
	)	
<b>v.</b>	)	<b>Criminal No. 11-10260-NMG</b>
	)	
<b>AARON SWARTZ,</b>	)	
<b>Defendant</b>	)	

**GOVERNMENT'S RESPONSE TO DEFENDANT'S  
MOTION TO COMPEL DISCOVERY**

The Court should deny the Defendant's motion to compel discovery.

The Government stands ready to produce the balance of automatic discovery once a protective order is in place. In fact, Exhibit 1 to Defendant's motion to compel discovery reflects the Government's willingness to produce most of the items identified in Defendant's motion to compel. As a precondition, however, this Court should put in place effective safeguards to prevent potentially irreparable and significant harm to the victims in this case by misuse of the discovery materials. The Government's proposed protective order strikes a careful balance between the risks of further harm to victims and the convenience of the defense in accessing sensitive materials. Once the Court resolves the nature and scope of an appropriate protective order, the materials will be produced without need of further intervention by the Court.

Defendant's motion to compel also seeks materials beyond those required by automatic discovery rules. To that extent, the Local Rules have a mechanism for requests for discovery: L.R. 116.3, which requires a defendant to request discovery by *letter* before filing a motion "[e]xcept in an emergency." This process was intended to avoid motion practice such as this.

The Court should consider a discovery motion only if Rule 116.3's process of consultation and the exchange of letters does not lead to a satisfactory resolution. This was the process the Government followed when seeking to negotiate a protective order.

Defendant did not follow this rule here. In particular, Defendant has not previously requested from the government:

- (1) Written statements by Defendant which are not relevant to the prosecution of this case and therefore not encompassed by Rule 16(a)(1)(B), such as certain Twitter postings, postings on his own website, text messages and electronic mail (requested in Item 1);
- (2) Complete video recordings, including extraneous time periods which will not be offered at trial and therefore are not encompassed by Rule 16 (E) (requested in Item 5);
- (3) The name of the student who identified Defendant from the photo array, whose name was appropriately redacted from the public record for purposes of privacy (requested in Item 6); and
- (4) E-mail references and network flow data from Defendant's own computer which he claims to be exculpatory evidence, but actually is not (requested in Item 7).

To expedite discovery, the Government proposes that the Court deny Defendant's motion to compel as unripe, and that the Government be allowed to treat Defendant's motion to compel as the type of discovery letter mandated by Local Rule 116.3, and to respond to the request by letter in accordance with the Rule. We anticipate most, if not all, discovery matters can be worked out with defense counsel through the process mandated by the Local Rules once a protective order is in place.

Respectfully submitted,

Carmen M. Ortiz  
United States Attorney

By: /s/ Stephen P. Heymann  
Stephen P. Heymann  
Scott L. Garland  
Assistant U.S. Attorneys

CERTIFICATE OF SERVICE

I hereby certify that these documents are being filed through the ECF system and therefore will be sent electronically to the registered participants as identified on the Notice of Electronic Filing.

/s/ Stephen P. Heymann  
Stephen P. Heymann  
Assistant U.S. Attorney

Date: October 6, 2011



MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4076916@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Set/Reset Hearings  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 10/6/2011 at 5:23 PM EDT and filed on 10/6/2011

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** No document attached

**Docket Text:**

**Set/Reset Hearings as to Aaron Swartz Discovery Hearing set for 10/11/2011 11:00 AM in Courtroom 15 before Ch. Magistrate Judge Judith G. Dein. (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Andrew Good agood@goodcormier.com, hill@goodcormier.com, josh@goodcormier.com,  
lpetrova@goodcormier.com, pcormier@goodcormier.com

Scott Garland scott.garland@usdoj.gov, janet.smith@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4085871@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Motion Hearing  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 10/13/2011 at 5:21 PM EDT and filed on 10/11/2011

**Case Name:** USA v. Swartz  
**Case Number:** 1:11-cr-10260-NMG  
**Filer:**  
**Document Number:** No document attached

**Docket Text:**

**ELECTRONIC Clerk's Notes for proceedings held before Ch. Magistrate Judge Judith G. Dein:** Motion Hearing as to Aaron Swartz held on 10/11/2011 re [19] MOTION to Compel Discovery filed by Aaron Swartz, [18] MOTION for Protective Order filed by USA; USMJ Dein hears arguments from Dft., Govt. and victims counsel(Feigelson); supplemental filings are due 10/24/11 and further hearing is set for 11/2/11 @ 2:30pm. (Attorneys present: Garland and Good and Feigelson )Court Reporter Name and Contact or digital recording information: Digital Recording. (Quinn, Thomas)

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Andrew Good agood@goodcormier.com, hill@goodcormier.com, josh@goodcormier.com, lpetrova@goodcormier.com, pcormier@goodcormier.com

Scott Garland scott.garland@usdoj.gov, janet.smith@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4089058@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Terminate Deadlines and Hearings  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 10/17/2011 at 10:40 AM EDT and filed on 10/17/2011

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** No document attached

**Docket Text:**

**Terminate Deadlines and Hearings as to Aaron Swartz: Discovery Hearing. (Moore, Kellyann)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Andrew Good agood@goodcormier.com, hill@goodcormier.com, josh@goodcormier.com,  
lpetrova@goodcormier.com, pcormier@goodcormier.com

Scott Garland scott.garland@usdoj.gov, janet.smith@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 11-10260-NMG
	)	
AARON SWARTZ,	)	
	)	
Defendant	)	

REPORT TO THE COURT RE DISCOVERY

At the hearing on October 11, 2011, concerning the Government's Motion for a Protective Order and the defendant's contemporaneous Motion to Compel Discovery, the Court asked the government to report back:

- (1) Whether it was possible to provide the defense metadata associated with files the defendant downloaded from JSTOR, without the valuable files themselves; and
- (2) Which categories of discovery materials the Government proposed the defendant be able to review only in his counsel's office, given the Court's preliminary ruling that those categories should be limited.

This report addresses those questions.

The Metadata

The database stolen by the defendant from JSTOR is contained on five hard drives and consists of approximately 4.85 million, unique .pdf documents. The Government has collected metadata for each of the downloaded documents, including the document's file name, size, location, when it was created, last written and modified. The metadata and uniquely identifying hash values (the equivalent of a "digital fingerprints") for the downloaded documents are being mailed to the defendant today in an electronically searchable, .txt format.

The Narrow Categories

At the hearing, the Court expressed its desire to limit the materials that the defendant would be required to view at his counsel's office, and asked the Government to review the discovery materials for this purpose. Having reviewed the discovery and consulted with victims, the Government has identified three categories:

- (1) Two e-mail chains containing discussions of security weaknesses in MIT's computer network;
- (2) Seven e-mail chains (or portions of chains) containing discussions of security methods of and weaknesses in JSTOR's network; and
- (3) Police reports containing the name of one student who identified the defendant from a photo spread, and one non-law enforcement witness, who has been charged but not convicted in state court in a matter arising out of a personal relationship.

An example of an e-mail from each of the two categories of vulnerabilities is being provided to the Court under seal for its review.

The sensitivity of the two categories of emails that the Government proposes to restrain are self-evident. The e-mails' release over the Internet, by any means, for any purpose, or by any individual, would invite further victimization of MIT and JSTOR and facilitate that victimization. The number of e-mails is modest: they have been selected after a careful and particularized review, and will not impose any meaningful burden on the defendant to review in his counsel's office.

The Government understands that the Court intends to enter a protective order limiting the use of discovery materials to use solely and exclusively to litigate this case, and not for any other purpose. Subject to such a protective order, the Government has no objection to providing the names of the student and the witness to the defense at this time. A redacted form of the

identification reports already has been provided to the defendant and redacted police reports relating to the witness will be provided as soon as the protective order is in place. By separating the name from these reports, the Government to prevent undue embarrassment to these witnesses, or targeting of them by third parties, should the police reports make their way to the Internet, again, by any means, for any purpose, or by any individual.

Respectfully submitted,

Carmen M. Ortiz  
United States Attorney

By: Stephen P. Heymann  
STEPHEN P. HEYMANN  
SCOTT L. GARLAND  
Assistant U.S. Attorneys

Date: October 24, 2011

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing.

Stephen P. Heymann  
Stephen P. Heymann  
Assistant United States Attorney

Date: October 24, 2011

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Crim. No. 11-CR-10260-NMG
	)	
AARON SWARTZ,	)	
Defendant	)	

**DEFENDANT AARON SWARTZ'S SUPPLEMENTAL  
SUBMISSION IN SUPPORT OF HIS MOTION  
TO COMPEL DISCOVERY AND A PROTECTIVE ORDER**

Aaron Swartz provides this supplemental submission to address certain issues raised during the October 11, 2011 hearing. The Court identified two categories of discoverable data:

- (1) the data allegedly downloaded from JSTOR's website; and
- (2) nine email chains of communications between MIT and JSTOR about the downloading and vulnerabilities that allegedly enabled or might enable downloading to occur.

**I. THE DOWNLOADED DATA.**

**A. Security Arrangements.**

Both in its motion seeking a protective order and at the hearing, the government attempts to justify an order that the defense be required to use the downloaded data to litigate this case and prepare for trial solely in a Secret Service office. Its insistence on keeping the data solely in the government's possession is based on a claim that "The government can secure this data to an extent that a law office cannot." Motion of the United States for a Protective Order, Dkt 18, at 3. The government claims that it is primarily concerned with preventing third parties from obtaining access to the

downloaded data. *Id.* It agrees that the defense counsel and its experts and investigators can be trusted to use the data lawfully. It has presented no evidence that Mr. Swartz cannot be similarly trusted to use the information exclusively for the defense of this case. Neither the government nor the Court can deny that Mr. Swartz is the most important member of the defense team who must examine and analyze discoverable data, including the downloaded data.

The government cannot and does not deny that the defense's searches and other work with the downloaded data is privileged information. The defense's selection of searches and other examinations of the downloaded data would be recorded in electronic data that would remain in the government's possession. For that reason, if its proposed protective order is approved by the Court, the government would have impermissible and unconstitutional access to the defense's work product-protected data. *See United States v. Horn*, 29 F.3d 754, 757-758 (1st Cir. 1994)(government surveillance of defense's selections from discoverable documents constitutes prosecutorial conduct).

The defense proposes that the downloaded data be provided to it at the offices of Collora LLP, which is on the 12<sup>th</sup> floor of the Federal Reserve Bank Building in Boston. That building and office is at least as secure as any other government building and office in Boston, including the US Attorney's office and the Secret Service office. The downloaded data would be stored in a locked space within the Collora LLP office suite. The keys would be possessed exclusively by undersigned counsel and William Kettlewell, a Collora LLP partner who was a consultant on the defense team prior to the indictment who met with the government and undersigned counsel prior to the indictment, and remains a member of the defense team without having filed his



appearance. Mr. Kettlewell is willing to sign a protective order, as are the defendant and all members of the defense team. The data would be stored and accessible only on an off-line computer at Collora LLP that is not connected to the Internet. In the event that the defense contends that it is necessary to modify the restrictions on storage, access and use of the downloaded data, the defense would be required to seek court approval. Terms for such a protective order are attached hereto as Exhibit 1.

**B. Severance of Metadata From Articles and Other Text.**

At the hearing, the Court ordered the government to inform the Court whether it is feasible to sever the metadata from the articles to which the metadata relates. The government has informed the defense counsel that it proposes to provide the defense with the metadata without the pdf files to which the metadata relates. The defense is entitled to, and must have, the same full set of downloaded data, including the pdf files that the government has, in order to litigate this case through a trial. Without the articles and other pdf files, the defense cannot effectively and efficiently conduct its analysis of exactly what was downloaded from where and under what circumstances. The metadata alone does not provide this essential set of full information. In view of the security arrangements proposed by the defense, there is no justification for redacting discoverable data and subjecting the defense to an unconstitutional burden of having to seek essential information about the downloaded data from the government. These defense requests would, in turn, disclose work product privileged information. The defense cannot be required to conduct this litigation without information that Rule 16 entitles it to have in order to provide even-handed access to evidence and information.

## **II. THE NON-DOWNLOADED DATA.**

The government proposes that Mr. Swartz be prohibited from receiving copies of nine email chains. Instead, it proposes that Mr. Swartz read, and work at his counsel's office with, these nine email chains pertaining to "security weaknesses" of MIT's and JSTOR's computer networks. Mr. Swartz is willing to sign a protective order restricting his use of this information to the litigation of this case. That is all that is necessary to provide a more than sufficient assurance against any improper or unlawful use of copies of these email chains.

The defense team, including Mr. Swartz, his lawyers, investigators and experts, are located in several cities, only one of which is Boston. Communication of privileged information within the defense camp occurs by password-protected, confidential email. Arguendo, even if the government's mistrust of Mr. Swartz is taken at face value, its proposal does not afford any substantial security against improper use of this discoverable information. Mr. Swartz must and will have all of the information in these nine email chains. These emails about means of access to MIT and JSTOR networks, characterized by the government as "vulnerabilities," may contain important exculpatory information, or may lead to exculpatory evidence. There is no basis in this record for Mr. Swartz to be the only member of the defense team who can have this information, but cannot have copies, to use for his defense.

Mr. Swartz must be able to make notes and send memoranda to the defense team about these nine emails after studying them up to and including the trial. He is not usually in Boston during the work week. He must work on this case on nights and

weekends. As to these nine email chains, the defense would transmit them as password-protected documents sent by electronic mail. The defense is willing to password protect these particular discovery materials by circulating them electronically among members of the defense team as provided in Exhibit 1.

In any event, based on this record, this Court should view with skepticism the government's unsupported claim that disclosure of the nine email chains threatens harm to either MIT or JSTOR. There is no affidavit or evidence in any form to support that claim. JSTOR's counsel did not express concern about any non-downloaded data including its communications with MIT or anyone else. MIT has not objected to disclosure of this supposedly sensitive information either. Even if MIT or JSTOR objected to disclosure, these documents are putative evidence that the defense may be entitled to admit during Mr. Swartz's public trial. Because these documents are potential evidence in a public trial, refusing to make copies available to Mr. Swartz cannot be justified. The government has abandoned its claim that Mr. Swartz cannot be trusted to have a copy of three lines of code he allegedly wrote and used to download data. It has unjustifiably withheld huge amounts of discoverable data for weeks by making wildly unsupported security claims that it has now abandoned. Mr. Swartz should have copies of the nine email chains exclusively for his use in defending this case.

### **III. THE SEIZED DATA, DEFENDANT'S STATEMENTS, AND EXCULPATORY EVIDENCE**

The Court should order the government to provide copies of the following:

- 1. Defendant's Written Statements.** The defendant's written statements that are within its custody, possession and control, e.g., Twitter and Facebook postings,

websites, text messages and electronic mail. The government obtained some of this information as the fruit of warrantless seizures of devices that the government asserts belong to Mr. Swartz; some are the fruit of warrant-authorized seizures of items that the government asserts belong to Mr. Swartz; and some information was obtained in response to grand jury subpoenas to electronic communications providers. The defendant's written statements are subject to automatic discovery. Local Rule 116.1(C)(1)(a) and Rule 16(a)(E). In paragraph A.1.a. of its August 12, 2011 letter to defense counsel (attached hereto as Exhibit 2), the government states that it will offer some of these written statements in its case-in-chief. The defendant's written statements are also material to the defense. The government does not provide any "good cause" for withholding the defendant's written statements.

**2. Seized Electronic Data.** In its August 12, 2011 letter, the government listed the items containing electronic data stored in electronic data storage media that it has seized as follows:

- Acer laptop computer recovered at MIT
- Western Digital hard drive recovered at MIT\*
- HP USB drive seized from the defendant at the time of his arrest
- Apple iMac computer seized at Harvard
- Western Digital hard drive seized at Harvard
- HTC G2 cell phone seized during the search of the defendant's residence
- Nokia 2320 cell phone seized during the search of the defendant's residence
- Sony Micro Vault seized during the search of the defendant's residence

The government has no good cause to withhold copies of the seized electronic data, all of which is discoverable under Rule 16(a)(1)(E). For that reason, the

---

\* Search warrant applications for devices seized at MIT and Harvard allege probable cause to believe that these devices belong to Mr. Swartz and are evidence of the commission of the offenses charged in the indictment.

instant motion seeks an order compelling the government to provide the defense with copies in the form of bit-by-bit, mirror electronic images of all of the data natively stored on the above-listed electronic devices, including any and all metadata. In order to effectively defend himself against the indictment's allegations, Mr. Swartz is constitutionally entitled to an exact and complete copy of the discoverable electronically stored information in its native format so that he may examine and, if appropriate, contest the provenance and substance of that evidence. *See United States v. Briggs*, 2011 U.S. Dist. LEXIS 101415 (W.D.N.Y.).

**3. Complete Video Recordings.** Paragraph E of the government's August 12, 2011 letter states that it has provided copies of what it considers to be the "relevant portions" of video recordings made on January 4 and 6, 2011, in a wiring closet in the basement of MIT's Building 16. Under Rule 16, Mr. Swartz is entitled to full and complete copies of all video recordings made in that closet including but not limited to recordings made at any time including, but not limited to, January 4 and 6, 2011, because the complete records contain evidence that is material to his defense.

**4. Exculpatory Evidence.** In paragraph H of the government's letter, the government described but refused to provide almost all of certain exculpatory evidence, including evidence that, during the period covered by the indictment, persons other than Mr. Swartz at Harvard, MIT and China accessed the Acer laptop that was seized by the government, and persons other than Mr. Swartz at MIT and elsewhere were engaging in "journal spidering" of JSTOR data using a "virtual computer" that can be hosted by anyone at MIT. The government has no

basis for withholding the electronic evidence described as exculpatory in its letter.

**CONCLUSION.**

For all the foregoing reasons, the Court should enter the order attached hereto as Exhibit 1.

Respectfully submitted,

/s/Andrew Good

Andrew Good

BBO # 201240

Good & Cormier

83 Atlantic Avenue

Boston, MA 02110

Tel. 617-523-5933

agood@goodcormier.com

**CERTIFICATE OF SERVICE**

I hereby certify that the foregoing document filed through the ECF system will be sent to counsel for the government who are registered participants as identified on the Notice of Electronic Filing ("NEF").

DATED: October 24, 2011

/s/ Andrew Good

Andrew Good

# **Exhibit 1**

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Crim. No. 11-CR-10260-NMG
	)	
AARON SWARTZ,	)	
Defendant	)	

**(PROPOSED) ORDER**

After consideration of the Government's motion for a protective order, the Defendant's motion to compel discovery, and the oppositions filed by both parties in response to the motions, it is ordered that the Government shall provide copies, or enable the Defendant to make copies, of the following that are within its possession, custody or control:

1. All electronic data that constitutes or includes a written statement of Mr. Swartz including communications on Twitter, Facebook, text message and email or any other form of electronic communication.
2. All data, documents, and tangible things including, but not limited to, data obtained from MIT and JSTOR, that are discoverable under Rule 16(a)(1)(E).

All data includes: (A) all data seized from devices that the government has asserted belong to the defendant, including:

- Acer laptop computer recovered at MIT
- Four Samsung hard drives delivered to the Secret Service by Defendant Swartz and his counsel on June 7, 2011
- Western Digital hard drive recovered at MIT\*
- HP USB drive seized from the defendant at the time of his arrest
- Apple iMac computer seized at Harvard

---

\* Search warrant applications for devices seized at MIT and Harvard allege probable cause to believe that these devices belong to Mr. Swartz and are evidence of the commission of the offenses charged in the indictment.



- Western Digital hard drive seized at Harvard
- HTC G2 cell phone seized during the search of the defendant's residence
- Nokia 2320 cell phone seized during the search of the defendant's residence
- Sony Micro Vault seized during the search of the defendant's residence

(B) All data and items that are material to preparing the defense, namely, all data and items that constitute, or are evidence of, the occurrences and activity, including electronic communications, transmissions, and activity, that the government alleges occurred in the indictment.

(C) All data and items that the government intends to use in its case-in-chief.

(D) With respect in particular to any and all data that the government alleges was illegally downloaded from JSTOR's database including, but not limited to the data stored in the Four Samsung hard drives delivered to the Secret Service by Defendant Swartz and his counsel on June 7, 2011 ("the downloaded data"), the government shall provide one bit by bit copy of the downloaded data in its native format to the defense at the office of Collora LLP, 400 Atlantic Avenue, Boston, into the custody of Attorney William Kettlewell who shall sign a copy of this order. Access to the room in which the downloaded data shall be stored at Collora LLP shall be controlled by keys to be kept in the sole custody of Mr. Kettlewell and Andrew Good. The downloaded data in the custody of Mr. Kettlewell and Mr. Good shall be accessed solely on an offline computer that is not connected to the internet. Until and unless this Court approves a written modification of this order, each member of the defense, including Mr. Swartz, may have access to the

downloaded data in the offices of Collora LLP, and at no other location, and only after signing a copy of this order.

(E) In the event that the defense electronically transmits copies of any or all of the nine email chains designated by the government by means of any form of internet communication including email, access to copies of any of the nine email chains must be protected by a privileged password.

3. All data, documents, and tangible things that constitute or are evidence of the potentially exculpatory information described in paragraph H.1 and H.5 of the government's August 12, 2011 letter to defense counsel other than the fingerprint data that has already been produced.
4. Full and complete copies of all video recordings made inside the closet in the basement of MIT Building 16 including, but not limited to, recordings made on January 4 and 6, 2011.
5. All data, documents, and tangible things that constitute or are evidence of the eyewitness identification procedure mentioned in paragraph G of the government's August 12, 2011 letter to defense counsel.

When the data referred to in this order is computerized electronic data, transmissions, or communications, the government shall provide copies, or enable the defense to make copies, of the data in its native, bit-by-bit form, including all metadata, if the government has the data in its native format including all metadata. If the government does not have the data in its native form, including all metadata, it is to provide copies or enable the defense to make copies in the same computer searchable format of the data that is within in the possession, custody and control of the government, including optical

character recognition software format.

Any and all documents and information provided to Mr. Swartz, his counsel, his counsel's investigators and defense are to be used solely for the litigation of this case and no part of the documents or information may be disclosed or used for any other purpose.

SO ORDERED.

Date:

---

JUDITH G. DEIN  
United States Chief Magistrate Judge

# **Exhibit 2**



**U.S. Department of Justice**

***Carmen M. Ortiz***  
*United States Attorney*  
*District of Massachusetts*

---

*Main Reception: (617) 748-3100*

*United States Courthouse, Suite 9200*  
*1 Courthouse Way*  
*Boston, Massachusetts 02210*

August 12, 2011

Mr. Andrew Good  
Good and Cormier  
83 Atlantic Avenue  
Boston, MA 02110

Re: United States v. Aaron Swartz  
Criminal No. 11-CR-10260

Dear Counsel:

Pursuant to Fed. R. Crim. P. 16 and Rules 116.1(C) and 116.2 of the Local Rules of the United States District Court for the District of Massachusetts, the government provides the following automatic discovery in the above-referenced case:

A. Rule 16 Materials

1. Statements of Defendant under Rule 16 (a)(1)(A) & (a)(1)(B)

a. Written Statements

The defendant's booking sheet and fingerprint card from the Cambridge Police Department are contained on enclosed Disk 5.

There are numerous relevant statements not made to government agents drafted by Defendant Swartz before the date of his arrest contained in electronic media, such as Twitter postings, websites and e-mail. These are equally available to the defendant. Those that the government intends to use in its case-in-chief are available for your review, as described in paragraph A(3) below.

Subject thereto, there are no relevant written statements of Defendant Swartz made

following his arrest in the possession, custody or control of the government, which are known to the attorney for the government.

b. Recorded Statements

The defendant made recorded statements at the time of his booking by Cambridge Police on January 6, 2011. A copy of his booking video is enclosed on Disk 7.

c. Grand Jury Testimony of the Defendant

Defendant Aaron Swartz did not testify before a grand jury in relation to this case.

d. Oral Statements to Then Known Government Agents

Defendant Aaron Swartz made oral statements at the time of the search of his apartment to individuals known to him at the time to be government agents. The only statements made by him then which the government believes at this time to be material are memorialized in the affidavit in support of the search warrant for his office at Harvard, a copy of which affidavit is enclosed on Disk 3.

2. Defendant's Prior Record under Rule 16 (a)(1)(D)

Enclosed on Disk 3 is a copy of the defendant's prior criminal record.

3. Documents and Tangible Objects under Rule 16(a)(1)(E)

All books, papers, documents and tangible items which are within the possession, custody or control of the government, and which are material to the preparation of the defendant's defense or are intended for use by the government as evidence in chief at the trial of this case, or were obtained from or belong to the defendant, may be inspected subject to a protective order by contacting the undersigned Assistant U.S. Attorney and making an appointment to view the same at a mutually convenient time.

Because many of these items contain potentially sensitive, confidential and proprietary communications, documents, and records obtained from JSTOR and MIT, including discussion of the victims' computer systems and security measures, we will need to arrange a protective order with you before inspection. Please review the enclosed draft agreement and let us know your thoughts.

4. Reports of Examinations and Tests under Rule 16 (a)(1)(F)

Enclosed you will find Disks 1, 2, 5 & 6 containing reports of examination of the following:

- Acer laptop computer recovered at MIT
- Western Digital hard drive recovered at MIT
- HP USB drive seized from the defendant at the time of his arrest
- Apple iMac computer seized at Harvard
- Western Digital hard drive seized at Harvard
- HTC G2 cell phone seized during the search of the defendant's residence
- Nokia 2320 cell phone seized during the search of the defendant's residence
- Sony Micro Vault seized during the search of the defendant's residence
- Four Samsung hard drives delivered to the Secret Service by Defendant Swartz and his counsel on June 7, 2011 (Please note that because of the number of files contained on Samsung model HD154UI hard drive, serial number S1Y6J1C2800332, it has not been practicable to date to make a complete file list in an Excel readable format, unlike the other drives.)
- A fingerprint analysis report from the Cambridge Police Department with respect to the Acer Laptop and Western Digital hard drive recovered at MIT
- A supplemental fingerprint analysis report with respect to these items

While not required by the rules, intermediate as well as final forensic reports where available are enclosed for many of the recovered and seized pieces of equipment on Disks 6 and 1, respectively.

B. Search Materials under Local Rule 116.1(C)(1)(b)

Search warrants were executed on multiple pieces of electronic equipment and at multiple locations. Copies of the search warrants, applications, affidavits, and returns have already been provided to you, but are further found on Disk 3.

Four Samsung Model HD154UI hard drives were examined following their consensual and unconditional delivery to the United States Secret Service on June 7, 2011. As an additional precaution, a warrant, enclosed on Disk 3, was also obtained.

C. Electronic Surveillance under Local Rule 116.1(C)(1)(c)

No oral, wire, or electronic communications of the defendant as defined in 18 U.S.C. § 2510 were intercepted relating to the charges in the indictment.

D. Consensual Interceptions under Local Rule 116.1(C)(1)(d)

There were no interceptions (as the term "intercept" is defined in 18 U.S.C. § 2510(4)) of wire, oral, or electronic communications relating to the charges contained in the indictment, made with the consent of one of the parties to the communication in which the defendant was intercepted or which the government intends to offer as evidence in its case-in-chief.

E. Video Recordings

On January 4, 2011 and January 6, 2011, Defendant Aaron Swartz was recorded entering a restricted wiring closet in the basement of MIT's Building 16. Copies of relevant portions of the recordings (where he is seen entering, in, or exiting the closet) are enclosed on Disk 4.

F. Unindicted Coconspirators under Local Rule 116.1(C)(1)(e)

There is no conspiracy count charged in the indictment.

G. Identifications under Local Rule 116.1(C)(1)(f)

Defendant Aaron Swartz was a subject of an investigative identification procedure used with a witness the government anticipates calling in its case-in-chief involving a photospread documented by MIT Police Detective Boulter. Relevant portions of the police report of Detective Boulter and a copy of the photospread used in the identification procedure are enclosed on Disk 3. In both instances, the name of the identifying MIT student has been redacted to protect the student's continuing right to privacy at this initial stage of the case. On page 2 of the Report of Photo Array, USAO-000007, the initials beside each of the enumerated items have been redacted for the same reason.

H. Exculpatory Evidence Under Local Rule 116.2(B)(1)

With respect to the government's obligation under Local Rule 116.2(B)(1) to produce "exculpatory evidence" as that term is defined in Local Rule 116.2(A), the government states as follows:

1. The government is unaware of any information that would tend directly to negate the defendant's guilt concerning any count in the indictment. However, the United States is aware of the following information that you may consider to be discoverable under Local Rule 116.2(B)(1)(a):
  - Email exchanges between and among individuals at MIT and JSTOR as they sought to identify the individual responsible for massive downloads on the dates charged in the Indictment. While the defendant has admitted to being responsible for the downloads and produced one copy of most of what was downloaded on these dates, these e-mails reflect JSTOR's and MIT's initial difficulties in locating and identifying him in light of the furtive tactics he was employing. The email exchanges will be made available in accordance with paragraph (A)(3) above.
  - Counsel for the government understands that a number of external connections were made and/or attempted to the Acer laptop between January 4, 2011 and January 6, 2011, including from a Linux server at MIT and from China. The Linux server was connected to a medical center at Harvard periodically during the same period. While government



counsel is unaware of any evidence that files from JSTOR were extracted by third parties through any of these connections, the connection logs will be made available to you in accordance with paragraph (A)(3) above.

- An analysis of one of the fingerprints on the Acer laptop purchased and used by the defendant cannot exclude his friend, Alec Resnick. The analysis is being produced for you; see paragraph (A)(4) above.
- While not a defense or material, one or more other people used or attempted to use scrapers to download JSTOR articles through MIT computers during the period of Defendant Swartz's illegal conduct. On the evening of November 29, 2010, the network security team at MIT was contacted and investigated journal spidering occurring on the site of the Institute of Electrical and Electronic Engineers. It was tracked to a group of shared computers on which anyone at MIT can host a virtual machine. It was determined that a virtual machine had been compromised. The user was notified that scripts placed on it were downloading journals from JSTOR, IEEE and APS. The machines were taken offline early the morning of November 30, 2010.
- The login screen on the Acer laptop when observed by Secret Service Agent Pickett on January 4, 2011 identified the user currently logged in as "Gene Host." A user name is different from a host name, and accordingly is similarly immaterial.

2. The government is unaware of any information that would cast doubt on the admissibility of evidence that the government anticipates offering in its case-in-chief and that could be subject to a motion to suppress or exclude.

3. Promises, rewards, or inducements have been given to witness Erin Quinn Norton. Copies of the letter agreement with her and order of immunity with respect to her grand jury testimony are enclosed on Disk 3.

4. The government is aware of one case-in-chief witness who has a criminal record.

Please be advised that one of the government's prospective trial witnesses was the subject of a charge in Somerville District Court in 1998 of being a minor in possession of alcohol and that the case was dismissed the following month upon payment of court costs. The government intends to make no further disclosures with respect to this matter, as the criminal charge could have no possible admissibility under either Fed.R.Crim.P. 609 or 608(b). If you believe you are entitled to additional information, including the identity of the prospective witness, please advise the undersigned, in which event the government will seek a protective order from the court to permit non-disclosure.

5. The government is aware of one case-in-chief witnesses who has a criminal case pending.

Please be advised that one of the government's prospective trial witnesses has pending state charges brought on July 7, 2009, involving the Abuse Prevention Act, Possession of Burglarious Tools, Criminal Harassment, and Breaking and Entering in the Daytime With Intent to Commit a felony. The events underlying the charges arise from the break-up of a personal relationship. The government has withheld the name of the witness and the others involved to protect their privacy, but will make them available along with the police reports in its possession subject to a protective order ensuring that the names, events and reports will not be disclosed publicly until the trial of this case, should the Court determine that a charge or information contained in the police reports is admissible for the purposes of cross-examination.

6. Based on the timeline as the government presently understands it from Officer Boulter's report described in paragraph G above and contained on Disk 3, no named percipient witnesses failed to make a positive identification of the defendant with respect to the crimes at issue. As reflected in the report, three students present when the Acer computer and Western Digital hard drive were recovered from Building 20 by law enforcement stated that they did not see anyone come in and place the computer there. However, as the timeline reflects, this was not a failed identification, but rather that they were not percipient witnesses to the event which had occurred earlier.

#### I. Other Matters

The government has preliminary analysis notes prepared at Carnegie Mellon of certain code and files contained on the Acer Laptop, as referenced on Page 2 of SA Michael Pickett's Forensic Cover Report contained on Disk 1. While these are not encompassed by Rule 16 (a)(1)(F) (formerly 16(a)(1)(D)), the government will make these available for review as described in section (A)(3), above, subject to the same procedures proscribed for preliminary transcripts in Local Rule 116.4 (B)(2).

Your involvement in the delivery of four hard drives containing documents, records and data obtained from JSTOR creates potential issues in this case under the Rules of Professional Conduct, as I am sure you are aware. To avoid the potential for those issues under Rule 3.7 in particular, we propose a stipulation from your client that the hard drives were from him, thus taking you out of the middle and rendering the origin an uncontested issue under the Rule. This stipulation would be without prejudice to all arguments on both sides as to the admissibility of the drives and their contents at any proceeding.

The government is aware of its continuing duty to disclose newly discovered additional evidence or material that is subject to discovery or inspection under Local Rules 116.1 and 116.2(B)(1) and Rule 16 of the Federal Rules of Criminal Procedure.

The government requests reciprocal discovery pursuant to Rule 16(b) of the Federal Rules of Criminal Procedure and Local Rule 116.1(D).

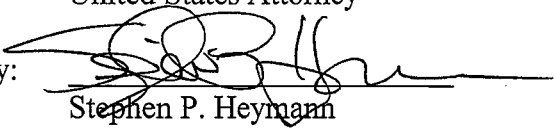
The government demands, pursuant to Rule 12.1 of the Federal Rules of Criminal Procedure, written notice of the defendant's intention to offer a defense of alibi. The time, date, and place at which the alleged offenses were committed is set forth in the indictment in this case a copy of which you previously have received.

Please call the undersigned Assistant U.S. Attorney at 617-748-3100 if you have any questions.

Very truly yours,

CARMEN M. ORTIZ  
United States Attorney

By:



Stephen P. Heymann  
Scott L. Garland  
Assistant U.S. Attorneys

enclosures

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
	)	
v.	)	Criminal No: 11-CR-10260-NMG
	)	
	)	
Aaron Swartz	)	
	)	

**Notice of Appearance**

Now comes the undersigned counsel and hereby enters his appearance on behalf  
of Aaron Swartz, the defendant in the above-captioned matter.

Respectfully Submitted,  
Aaron Swartz,  
By His Attorney,

**/s/ Martin G. Weinberg**  
Martin G. Weinberg, Esq.  
20 Park Plaza, Suite 1000  
Boston, MA 02116  
Tel: (617) 227-3700  
Fax: (617) 338-9538  
owlmgw@att.net

Dated: October 25, 2011

**Certificate of Service**

I, Martin G. Weinberg, hereby certify that on this date, October 25, 2011, a copy  
of the foregoing document has been served via CM/ECF Electronic Filing, upon  
Assistant U.S. Attorney Steven P. Heymann.

**/s/ Martin G. Weinberg**  
Martin G. Weinberg

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Crim. No. 11-CR-10260-NMG
	)	
AARON SWARTZ,	)	
Defendant	)	

**MOTION TO WITHDRAW AS COUNSEL FOR THE DEFENDANT**

Andrew Good, Philip Cormier and Good & Cormier move for leave to withdraw as counsel for Aaron Swartz. Substitute counsel, Martin Weinberg, has filed his notice of appearance.

Respectfully submitted,

/s/Andrew Good  
Andrew Good  
BBO # 201240  
Good & Cormier  
83 Atlantic Avenue  
Boston, MA 02110  
Tel. 617-523-5933  
agood@goodcormier.com

CERTIFICATE OF SERVICE

I hereby certify that the foregoing document filed through the ECF system will be sent to counsel for the government who are registered participants as identified on the Notice of Electronic Filing ("NEF").

DATED: October 27, 2011

/s/ Andrew Good  
Andrew Good

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4117528@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Motion Hearing  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 11/3/2011 at 3:47 PM EDT and filed on 11/2/2011

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** No document attached

**Docket Text:**

**ELECTRONIC Clerk's Notes for proceedings held before Ch. Magistrate Judge Judith G. Dein:** Motion Hearing as to Aaron Swartz held on 11/2/2011 re [24] MOTION Discovery order re [19] MOTION to Compel Discovery filed by Aaron Swartz, [19] MOTION to Compel Discovery filed by Aaron Swartz; USMJ Dein hears arguments from counsel and victim and continues hearing to 11/8/11 @ 2:30pm. (Attorneys present: Garland and Weinberg. ) Court Reporter Name and Contact or digital recording information: Digital Recording. (Quinn, Thomas)

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Andrew Good agood@goodcormier.com, hill@goodcormier.com, josh@goodcormier.com, lpetrova@goodcormier.com, pcormier@goodcormier.com

Scott Garland scott.garland@usdoj.gov, janet.smith@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4117547@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Order on Motion to Withdraw as Attorney  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 11/3/2011 at 3:50 PM EDT and filed on 11/3/2011

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** No document attached

**Docket Text:**

**Ch. Magistrate Judge Judith G. Dein: ELECTRONIC ORDER entered granting [26] Motion to Withdraw as Attorney Attorney Andrew Good terminated as to Aaron Swartz (1) (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Andrew Good agood@goodcormier.com, hill@goodcormier.com, josh@goodcormier.com, lpetrova@goodcormier.com, pcormier@goodcormier.com

Scott Garland scott.garland@usdoj.gov, janet.smith@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4121554@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Set/Reset Hearings  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 11/7/2011 at 2:16 PM EST and filed on 11/7/2011

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** No document attached

**Docket Text:**

**Set/Reset Hearings as to Aaron Swartz Discovery Hearing set for 11/8/2011 02:30 PM in Courtroom 15 before Ch. Magistrate Judge Judith G. Dein. (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, janet.smith@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**



MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4125120@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Motion Hearing  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 11/9/2011 at 9:43 AM EST and filed on 11/8/2011

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** No document attached

**Docket Text:**

**ELECTRONIC Clerk's Notes for proceedings held before Ch. Magistrate Judge Judith G. Dein:**Motion Hearing as to Aaron Swartz held on 11/8/2011 re [24] MOTION Discovery order re [19] MOTION to Compel *Discovery* filed by Aaron Swartz, [19] MOTION to Compel *Discovery* filed by Aaron Swartz; Counsel report they are working on an agreement on a protective order and the form which discovery will be produced.(Attorneys present: Garland and Weinberg. )Court Reporter Name and Contact or digital recording information: Digital Recording. (Quinn, Thomas)

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, janet.smith@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

CRIMINAL No.  
11-10260-NMG

UNITED STATES OF AMERICA

v.

AARON SWARTZ

**ORDER ON EXCLUDABLE TIME**

November 8, 2011

DEIN, M.J.

With the agreement of the parties, this court finds and concludes, pursuant to the provisions of 18 U.S.C. § 3161(h)(7)(A) and Section 5(b)(7)(B) of the Plan for Prompt Disposition of Criminal Cases in the United States District Court for the District of Massachusetts (Statement of Time Limits Adopted by the Court and Procedures for Implementing Them, Effective December 2008) that the defendant requires additional time for the preparation of an effective defense, including time for review of the evidence, preparation of motions and consideration of alternatives concerning how best to proceed, and that the interests of justice outweighs the best interests of the public and the defendant for a trial within seventy days of the return of an indictment, and that not granting this continuance would deny counsel for the defendant a reasonable time necessary for effective preparation. See 18 U.S.C. § 3161(h)(7)(B)(iv).

Accordingly, it is hereby ordered that the Clerk of this Court enter excludable time for the period of

November 2, 2011 through December 14, 2011,

that being the period between the expiration of the last order on excludable time and the next status conference.

Based upon the prior orders of the court dated July 19, 2011, September 9, 2011 and this order, at the time of the Interim Status Conference on December 14, 2011 there will be zero (0) days of non-excludable time under the Speedy Trial Act and seventy (70) days will remain under the Speedy Trial Act in which this case must be tried.

/ s / Judith Gail Dein  
JUDITH GAIL DEIN  
United States Magistrate Judge

**UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS**

**UNITED STATES OF AMERICA**

**v.**

**AARON SWARTZ,  
Defendant**

)  
)  
)  
)  
)  
)

**Criminal No. 11-10260-NMG**

**PROTECTIVE ORDER**

Whereas the Indictment in this case alleges that JSTOR and the Massachusetts Institute of Technology ("MIT") are victims of conduct committed by Defendant Aaron Swartz, and the materials discoverable in this case under Fed. R. Crim. P. 16 and L. R. 116.1-116.2 contain potentially sensitive, confidential and proprietary communications, documents, and records obtained from JSTOR and MIT, including discussion of the victims' computer systems and security measures,

The Court finds, without objection, good cause for entry of this Protective Order pursuant to Fed. R. Crim. P. 16(d):

1. The Government and the defense - that is, Defendant Swartz, his defense counsel and their staff, and any experts or investigators with whom defense counsel elects to consult- shall produce all documents, files and records discoverable under Fed. R. Crim. P. 16 and L.R. 116.1-116.2 ("discovery materials") for review in accordance with the conditions set by this Order.

2. With the exceptions listed below, the defense may obtain, make, and exchange amongst themselves copies of any discovery materials they deem necessary to prepare the defense of this case. All discovery materials and copies of discovery materials made by them or

provided to them by the Government shall be kept securely at their offices, residences, or while it is being reviewed in any other location

a. Per the parties' agreement, and without prejudice to a future application based on good cause by the defendant as set forth below, the Government will not, at this point, provide the defense complete imaged copies of all the files contained on four Samsung hard drives delivered to the Government by Defendant Aaron Swartz on June 17, 2011, and journal articles and other materials contained on a Maxtor hard drive seized by the Government at MIT on January 6, 2011. In lieu of the defense receiving complete copies of these hard drives:

i. The Government shall provide the defense electronic copies of those hard drives from which will be redacted all articles downloaded from JSTOR with the exception of approximately 350,000 separate articles that JSTOR released for free, public access on September 7, 2011, with those files' metadata intact in a form that will permit adequate forensic examination of the files. If this is not practicable, the parties shall work to agree on procedures to implement paragraph 2 (a) (v) (C) of this Order. The parties shall return to this Court with a proposed supplemental order and, if necessary, any disagreements they may have concerning sufficient security limitations carefully narrowed. All other aspects are severable and shall remain in full force and effect.

ii. The Government shall provide the defense a report listing all the files on the hard drives, along with the files' metadata.

iii. The Government shall provide the defense a bibliographic-type listing of the JSTOR articles found on the hard drives in sufficient detail to enable the defense to identify each such article.

iv. The Government shall make forensic copies of the complete unredacted hard drives available for review by the defense at the Boston Office of the Secret Service at reasonable times upon 7 day notice that any member of the defense wants to inspect or conduct forensic tests upon the hard drives. During any review conducted by the defense, the Secret Service shall make an agent otherwise unaffiliated with the investigation and prosecution of this case available to provide assistance. This agent shall not communicate with the prosecution team about what items the defense reviews and shall not be present during the viewing and/or testing, except at the defense's request or with prior approval of the Court. The parties will agree upon additional procedures necessary to ensure the security of the records and files stored on these hard drives in the event that the defense elects to do further inspection or conduct forensic examinations upon the hard drives at the Secret Service.

v. The defense shall not move for and the Court will not grant, an order requiring the Government to provide the defense copies of all the files on these hard drives, unless the defense demonstrates to the Court by a preponderance of the evidence that (A) defense counsel after inspection and forensic examination of the discovery materials provided pursuant to this agreement has a well founded basis, which will be particularized for the Court, that additional forensic testing on files other than those produced under subparagraph i, above, will lead to evidence material to the defense that cannot be adequately developed from the discovery materials provided pursuant to paragraphs 2 (a) (i-iii); or (B) the requested additional production is otherwise necessary to protect Defendant's constitutional rights; and (C) the defense's storage of and Defendant's access to all of these files will be under sufficiently secure restrictions to prevent the files' theft or public distribution (including restrictions on the location of the files'

storage, restrictions on who may have physical or electronic access to the files, the conditions under which Defendant can access the files, and the posting of substantial, third party financial security).

- b. Defendant may inspect, but may not be given or allowed to reproduce, copies of:
  - (1) Two e-mail chains identified by the Government containing discussions of security weaknesses in MIT's computer network;
  - (2) Seven e-mail chains (or portions of chains) identified by the Government containing discussions of security methods of and weaknesses in JSTOR's network; and
  - (3) Police reports containing the name of one student who identified the defendant from a photo spread, and one non-law enforcement witness, who has been charged but not convicted in state court in a matter arising out of a personal relationship.

Defense counsel will, however, receive unredacted email chains and police reports of the identification which the defendant may fully inspect without copying at counsel's office.

3. The Government and the defense shall use the opposing party's discovery materials solely and exclusively to litigate this case (including investigation, pre-trial motions, trial preparation, trial, and appeal), and not for any other purpose. In the event either party believes it necessary to use any such materials for any other purpose, they may seek leave of Court, in which instance opposing counsel and victims shall have an opportunity to be heard.

4. Except when preparing a potential witness, the defense shall not show or make the discovery materials available by any means (electronic, physical or otherwise) to any person who is not a member of the defense, absent further order of this Court. Once a potential witness has also signed and agreed to be bound by the terms of this Protective Order, the defense may show

the potential witness discovery materials necessary to prepare them, but may not give or allow the potential witness to retain the discovery materials or copies of them.

5. Each person receiving access to an opposing party's discovery materials other than counsel for the government, law enforcement officers, and counsel for the Defendant, shall first sign and date a copy of this Order to indicate their understanding of, acknowledgment of, and agreement to abide by its terms. Both the Government attorney and Defense counsel shall keep the signed copies in the event of a disclosure or use of discovery materials prohibited by this Order. Neither party shall be required to disclose to the other party who has been given access to what discovery materials, absent further order of this Court following an opportunity to be heard.

6. Defense counsel shall promptly notify the Government and this Court, and Government counsel shall promptly notify Defense counsel and this Court, if any discovery materials are (a) used in a manner inconsistent with this Order or (b) disclosed either intentionally or unintentionally to anyone not designated by this Order or further order of the Court. Each member of the defense and potential witness provided access to discovery materials shall promptly notify defense counsel of any such disclosures.

7. At the end of these proceedings, including any potential appeals, the defense shall destroy all copies of discovery materials received and made by it. Defense counsel may keep one copy of all discovery materials for such additional time as they deem necessary to ensure their ability to satisfy all professional obligations to Defendant in this matter. The Government may keep one copy of all defense discovery materials for such additional time as it deems necessary to satisfy its professional obligations and any relevant statutes, regulations, or policies.

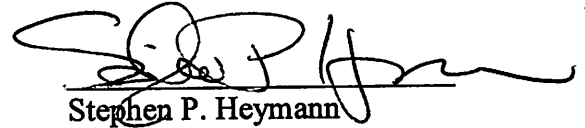


8. Nothing in this protective order is intended to otherwise restrict the proper use by the parties of any discovery materials during the investigation, pre-trial litigation, trial preparation, trial or appeal of this matter.

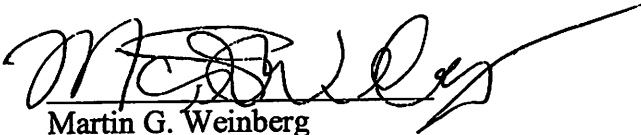
SO STIPULATED.



Aaron Swartz  
Defendant



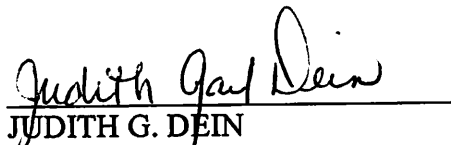
Stephen P. Heymann  
Scott L. Garland  
Assistant U.S. Attorneys



Martin G. Weinberg  
Defense Counsel

SO ORDERED.

Date: 11/30/11



JUDITH G. DEIN  
United States Chief Magistrate Judge

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4174206@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Status Conference by Magistrate Judge  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 12/14/2011 at 2:33 PM EST and filed on 12/14/2011

**Case Name:** USA v. Swartz  
**Case Number:** 1:11-cr-10260-NMG  
**Filer:**  
**Document Number:** No document attached

**Docket Text:**

**ELECTRONIC Clerk's Notes for proceedings held before Ch. Magistrate Judge Judith G. Dein: Status Conference as to Aaron Swartz held on 12/14/2011; Counsel report discovery is ongoing and seek further conference for 1/25/12 @ 10:00am(Attorneys present: Garland and Weinberg. )Court Reporter Name and Contact or digital recording information: Digital Recording – for transcripts or CDs contact Deborah Scalfani by email at [deborah\\_scalfani@mad.uscourts.gov](mailto:deborah_scalfani@mad.uscourts.gov). (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg [owlmcb@att.net](mailto:owlmcb@att.net), [owlmgw@att.net](mailto:owlmgw@att.net)

Stephen P. Heymann [Stephen.Heymann@usdoj.gov](mailto:Stephen.Heymann@usdoj.gov), [Jodi.gird@usdoj.gov](mailto:Jodi.gird@usdoj.gov), [usama.ecf@usdoj.gov](mailto:usama.ecf@usdoj.gov)

Scott Garland [scott.garland@usdoj.gov](mailto:scott.garland@usdoj.gov), [janet.smith@usdoj.gov](mailto:janet.smith@usdoj.gov), [jodi.gird@usdoj.gov](mailto:jodi.gird@usdoj.gov), [usama.ecf@usdoj.gov](mailto:usama.ecf@usdoj.gov)

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

CRIMINAL No.  
11-10260-NMG

UNITED STATES OF AMERICA  
v.

AARON SWARTZ

**INTERIM STATUS REPORT**

December 14, 2011

DEIN, M.J.

An Interim Status Conference was held before this court on Wednesday, December 14, 2011 pursuant to the provisions of Local Rule 116.5(A). Based on that conference, this court enters the following report and orders, to wit:

1. The defendant is in the process of reviewing the materials produced by the government to date. The parties have agreed on the terms of a confidentiality agreement.
2. The defendant has requested expert discovery, and the parties will submit a proposed schedule at the next status conference. Pursuant to the schedule, the government shall produce its expert discovery first, then the defendant, then an opportunity for the government to respond.
3. All dates for filing discovery and/or dispositive motions shall be set at the next status conference.
4. In this court's view, this is not a case involving unusual or complex issues for which an early joint conference of the district judge and the magistrate judge with counsel of record would be useful.
5. In this court's view, this is not a case involving features which would warrant special attention or modification of the standard schedule, except as provided herein.
6. The parties anticipate that there will be a trial, and that the government's case will take approximately 2 weeks.

7. This court finds and concludes, pursuant to the provisions of 18 U.S.C. § 3161(h)(7)(A) and Section 5(b)(7)(B) of the Plan for Prompt Disposition of Criminal Cases in the United States District Court for the District of Massachusetts (Statement of Time Limits Adopted by the Court and Procedures for Implementing Them, Effective December 2008) that the defendant requires additional time for the preparation of an effective defense, including time for review of the evidence, and consideration of alternatives concerning how best to proceed with this matter, and that the interests of justice outweighs the best interests of the public and the defendant for a trial within seventy days of the return of an indictment.

Accordingly, it is hereby ordered that the Clerk of this Court enter excludable time for the period of December 14, 2011 through January 25, 2012, that being the period between the expiration of the last order on excludable time and the next status conference.<sup>1</sup>

8. Based upon the prior orders of the court dated July 19, 2011, September 9, 2011, November 8, 2011 and the order entered contemporaneously herewith, at the time of the Interim Status Conference on January 25, 2012 there will be zero (0) days of non-excludable time under the Speedy Trial Act and seventy (70) days will remain under the Speedy Trial Act in which this case must be tried.
9. **An Interim Status Conference has been scheduled for January 25, 2012 at 10:00 a.m. Counsel for the respective parties shall file a Joint Memorandum addressing the matters set forth in LR 116.5(A)(1) through (7) before the close of business no less than THREE business days prior to that Status Conference. In addition, the parties shall include in the Joint Memorandum not only the periods of excludable time that are applicable, but also the amount of time remaining under the Speedy Trial Act before trial**

---

<sup>1</sup> The parties are hereby advised that under the provisions of Rule 2(b) of the Rules for United States Magistrates in the United States District Court for the District of Massachusetts, any party may move for reconsideration by a district judge of the determination(s) and order(s) set forth herein within ten (10) days after receipt of a copy of this order, unless a different time is prescribed by this court or the district judge. The party seeking reconsideration shall file with the Clerk of this Court, and serve upon all parties, a written notice of the motion which shall specifically designate the order or part thereof to be reconsidered and the basis for the objection thereto. The district judge, upon timely motion, shall reconsider the magistrate's order and set aside any portion thereof found to be clearly erroneous in fact or contrary to law. The parties are further advised that the United States Court of Appeals for this Circuit has indicated that failure to comply with this rule shall preclude further appellate review. See Keating v. Secretary of Health and Human Services, 848 F.2d 271 (1<sup>st</sup> Cir. March 31, 1988); United States v. Emiliano Valencia-Copete, 792 F.2d 4 (1<sup>st</sup> Cir. 1986); Park Motor Mart, Inc. v. Ford Motor Co., 616 F.2d 603 (1<sup>st</sup> Cir. 1980); United States v. Vega, 678 F.2d 376, 378-379 (1<sup>st</sup> Cir. 1982); Scott v. Schweiker, 702 F.2d 13, 14 (1<sup>st</sup> Cir. 1983); see also Thomas v. Arn, 474 U.S. 140, 106 S. Ct. 466 (1985).

**must commence,  
has been excluded.**

**as well as the total amount of time which**

      / s / Judith Gail Dein  
JUDITH GAIL DEIN  
UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

CRIMINAL No.  
11-10260-NMG

UNITED STATES OF AMERICA

v.

AARON SWARTZ

**ORDER ON EXCLUDABLE TIME**

December 14, 2011

DEIN, M.J.

With the agreement of the parties, this court finds and concludes, pursuant to the provisions of 18 U.S.C. § 3161(h)(7)(A) and Section 5(b)(7)(B) of the Plan for Prompt Disposition of Criminal Cases in the United States District Court for the District of Massachusetts (Statement of Time Limits Adopted by the Court and Procedures for Implementing Them, Effective December 2008) that the defendant requires additional time for the preparation of an effective defense, including time for review of the evidence, preparation of motions and consideration of alternatives concerning how best to proceed, and that the interests of justice outweighs the best interests of the public and the defendant for a trial within seventy days of the return of an indictment, and that not granting this continuance would deny counsel for the defendant a reasonable time necessary for effective preparation. See 18 U.S.C. § 3161(h)(7)(B)(iv).

Accordingly, it is hereby ordered that the Clerk of this Court enter excludable time for the period of

December 14, 2011 through January 25, 2012,

that being the period between the expiration of the last order on excludable time and the next status conference.

Based upon the prior orders of the court dated July 19, 2011, September 9, 2011, November 8, 2011 and this order, at the time of the Interim Status Conference on January 25, 2012 there will be zero (0) days of non-excludable time under the Speedy Trial Act and seventy (70) days will remain under the Speedy Trial Act in which this case must be tried.

          / s / Judith Gail Dein            
JUDITH GAIL DEIN  
United States Magistrate Judge

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 11-10260-NMG
	)	
AARON SWARTZ,	)	
	)	
Defendant	)	

MOTION TO RESCHEDULE INTERIM STATUS CONFERENCE  
AND FOR ORDER OF EXCLUDABLE DELAY

By order dated December 14, 2011, this Court scheduled the next status conference in this case for January 25, 2012 at 10:00 a.m. At that time, the Court planned to set all dates for filing discovery and/or dispositive motions. The Court also requested that counsel for the respective parties file a joint memorandum addressing the matters set forth in Local Rule 116.5(A), including whether a trial was anticipated and what date should be established for the final status conference and/or any other interim status conferences.

Since the last interim status conference, the government has redacted and produced to the defendant the four hard drives of materials contemplated by the agreed protective order. It has also continued to supplement its productions of those materials set forth in Rule 116.1(c).

The government has offered to, and the defendant has requested that the government, produce early many of the materials set forth in Local Rule 116.2(B)(2) and the Jencks Act. To accomplish this, the government is in the process of reviewing an extensive electronic database of materials. The parties believe that producing many of these materials early will enable the defense to better assess the case and any potential dispositive motions to be filed in it, will enable the parties to brief any contested matters for the Court with greater clarity, and is in the



interest of justice.

The parties request that the next interim status conference be postponed until the afternoon of March 15, 2012. At that time, the parties will better be able to assess whether any discovery motions are necessary, and how long the defense will require to review produced discovery materials before filing any dispositive motions they may deem appropriate.

The parties further request that the Court enter an order of excludable delay from January 25 through March 15, 2012 on the grounds that the defendant requires additional time for the preparation of an effective defense, including receipt and review of the supplemental materials being produced by the government, and consideration of alternatives concerning how best to proceed with this matter, and that the interest of justice outweigh the best interest of the public and the defendant for a trial within 70 days of the return of the indictment.

Respectfully submitted,

Carmen M. Ortiz  
United States Attorney

Martin G. Weinberg  
MARTIN G. WEINBERG, Esq.  
Counsel for Defendant Aaron Swartz

By: Stephen P. Heymann  
STEPHEN P. HEYMANN  
SCOTT L. GARLAND  
Assistant U.S. Attorneys

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

Stephen P. Heymann  
STEPHEN P. HEYMANN  
Assistant United States Attorney

Date: January 19, 2012

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4222620@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Order on Motion to Exclude  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 1/20/2012 at 4:50 PM EST and filed on 1/20/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** No document attached

**Docket Text:**

**Ch. Magistrate Judge Judith G. Dein: ELECTRONIC ORDER entered granting [31] Motion to Exclude as to Aaron Swartz (1); granting [31] Motion to Continue as to Aaron Swartz (1)( Status Conference set for 3/15/2012 02:00 PM in Courtroom 15 before Ch. Magistrate Judge Judith G. Dein.) (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

CRIMINAL No.  
11-10260-NMG

UNITED STATES OF AMERICA

v.

AARON SWARTZ

**ORDER ON EXCLUDABLE TIME**

January 20, 2012

DEIN, M.J.

The status conference, originally scheduled for January 25, 2012, has been continued to March 15, 2012 at 2:00 p.m. at the request of the parties, to enable all parties to further coordinate the production and review of the voluminous documents in this case. With the agreement of the parties, this court finds and concludes, pursuant to the provisions of 18 U.S.C. § 3161(h)(7)(A) and Section 5(b)(7)(B) of the Plan for Prompt Disposition of Criminal Cases in the United States District Court for the District of Massachusetts (Statement of Time Limits Adopted by the Court and Procedures for Implementing Them, Effective December 2008) that the defendant requires additional time for the preparation of an effective defense, including time for review of the evidence, preparation of motions and consideration of alternatives concerning how best to proceed, and that the interests of justice outweighs the best interests of the public and the defendant for a trial within seventy days of the return of an indictment, and that not granting this continuance would deny counsel for the defendant a reasonable time necessary for effective preparation. See 18 U.S.C. § 3161(h)(7)(B)(iv).

Accordingly, it is hereby ordered that the Clerk of this Court enter excludable time for the period of

January 25, 2012 through March 15, 2012,

that being the period between the expiration of the last order on excludable time and the next status conference.

Based upon the prior orders of the court dated July 19, 2011, September 9, 2011, November 8, 2011, December 14, 2011 and this order, at the time of the Interim Status Conference on March 15, 2012 there will be zero (0) days of non-excludable time under the Speedy Trial Act and seventy (70) days will remain under the Speedy Trial Act in which this case must be tried.

/ s / Judith Gail Dein  
JUDITH GAIL DEIN  
United States Magistrate Judge

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 11-10260-NMG
	)	
AARON SWARTZ,	)	
	)	
Defendant	)	

**ASSENTED TO MOTION FOR MODIFICATION OF  
CONDITIONS OF PRETRIAL RELEASE**

Now comes the defendant Aaron Swartz who hereby requests that this Honorable Court modify his conditions of release. As reason therefore, defendant states:

1. That he was released on July 19, 2011 on conditions memorialized in Chief Magistrate Judge Judith G. Dein's ORDER Setting Conditions of Release (Doc. 6) that included that he maintain his current residence in Cambridge, Massachusetts with travel restricted to the continental United States and that he report as directed by Pretrial Services;
2. That he is currently reporting in person every other week to Pretrial Services;
3. That he has fully complied with all the conditions of pretrial release through the current date;
4. That he is currently employed by Avaaz Foundation in New York;
5. That his employment requires that he relocate to a new address, [REDACTED] [REDACTED] [REDACTED] Brooklyn, New York [REDACTED];
6. That this change of residence will not interfere with his communications with counsel, their working together in meaningful pretrial preparation, or his counsel's ability in any way to prepare for trial;

7. That AUSA Stephen Heymann assents to the granting of this motion conditioned on the representations in paragraph 6, *supra*;
8. That Pretrial Services Officer Gina Affsa informed counsel that she had no objection to the transfer and that pretrial supervision would be transferred to the Eastern District of New York if the Court allows the motion

Respectfully submitted,  
Aaron Swartz,  
By His Attorney,

**/s/ Martin G. Weinberg**  
Martin G. Weinberg, Esq.  
MARTIN G. WEINBERG, P.C.  
Mass. Bar No. 519480  
20 Park Plaza, Suite 1000  
Boston, MA 02116  
Telephone: (617) 227-3700  
Facsimile: (617) 338-9538  
[owlmgw@att.net](mailto:owlmgw@att.net)

**Certificate of Service**

I, Martin G. Weinberg, hereby certify that on this date, February 1, 2012, a copy of the foregoing document has been served electronically via the CM/ECF system upon Assistant U.S. Attorneys Scott Garland and Stephen Heymann.

**/s/ Martin G. Weinberg**  
Martin G. Weinberg, Esq.

Date: February 1, 2012

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4246964@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Order on Motion to Modify  
Conditions of Release  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 2/7/2012 at 9:09 AM EST and filed on 2/7/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** No document attached

**Docket Text:**

**Magistrate Judge Judith G. Dein: ELECTRONIC ORDER entered granting [33] Motion to Modify Conditions of Release as to Aaron Swartz (1) (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 11-10260-NMG
	)	
AARON SWARTZ,	)	
	)	
Defendant	)	

JOINT MEMORANDUM IN ANTICIPATION OF INTERIM STATUS CONFERENCE

The Court has scheduled the next Interim Status Conference in this case for March 15, 2012. Pursuant to Local Rule 116.5(b), the parties jointly request that the Court waive this status conference and schedule one in 60 days, during the week of May 14, 2012. This period is necessary for the defense to review discovery materials it has received to date, to determine whether requests for additional discovery materials are necessary, and to consider alternatives of how best to proceed in this matter in light of its evaluation of the discovery materials.

The parties further request that the Court enter an order of excludable delay under the Speedy Trial Act from March 15, 2012 to the date set by the Court for the next Interim Status Conference on the grounds that the defendant requires additional time for the preparation of an effective defense, including time for review of the evidence, and consideration of alternatives concerning how best to proceed with this matter, and that the interests of justice outweighs the best interests of the public and the defendant for a trial within seventy days of the return of an indictment.

(1) The government has produced automatic discovery. In addition, the government has just provided early discovery of many but not all of the materials set forth in Local Rule 116.2(B)(2) and the Jencks Act in the form of a searchable electronic Concordance database.



(2) Additional discovery will be produced in accordance with the schedule established by the Local Rules of this Court, the Federal Rules of Criminal Procedure and by statute.

(3) The parties believe that early discovery provided by the government will enable the defense to better assess the case and any potential dispositive motions to be filed in it and will enable the parties to brief any contested matters for the Court with greater clarity. However, the defense reserves the right to make any additional discovery requests that are appropriate after review of the materials it has received from the government prior to the next scheduled Interim Status Conference.

(4) A protective order has been entered by the Court in this case.

(5) There are no pending pretrial motions under Fed. R. Crim. P. 12(b). The parties request that the Court defer setting a schedule for the filing of dispositive motions in this case until the next Interim Status Conference in order to give the defense a sufficient opportunity to review the substantial discovery it has received.

(6) The parties propose that expert witness disclosure in this case take place in three phases. The government will make its initial expert witness disclosure 11 weeks before trial. The defense will make theirs 8 weeks before trial. The government may then make an additional expert disclosure 5 weeks before trial, if an additional expert or experts are necessary to address matters raised in the defense disclosure.

(7) The defenses of insanity, public authority and alibi have not been raised in this case.

(8) The Court should exclude the period from March 15, 2012 through the date of the next Interim Status Conference under the Speedy Trial Act.

(9) The parties believe that trial is likely and that the trial will last around 3 weeks.

(10) The parties request that the next Interim Status Conference be set for the week of May 14, 2012, in approximately 60 days.

Respectfully submitted,

Carmen M. Ortiz  
United States Attorney

Martin G. Weinberg  
MARTIN G. WEINBERG, Esq.  
Counsel for Defendant Aaron Swartz

By: Stephen P. Heymann  
STEPHEN P. HEYMANN  
SCOTT L. GARLAND  
Assistant U.S. Attorneys

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

Stephen P. Heymann  
STEPHEN P. HEYMANN  
Assistant United States Attorney

Date: March 8, 2012

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

CRIMINAL No.  
11-10260-NMG

UNITED STATES OF AMERICA  
v.

AARON SWARTZ

**INTERIM STATUS REPORT**

March 16, 2012

DEIN, M.J.

An Interim Status Conference was scheduled to be held before this court on March 15, 2012 pursuant to the provisions of Local Rule 116.5(b), but the parties submitted a Joint Memorandum and the court waived the conference. Based on that Joint Memorandum, this court enters the following report and orders, to wit:

1. The government has produced its automatic discovery as well as additional materials, and defendant is in the process of reviewing the materials produced by the government to date.
2. Any additional discovery will be produced in accordance with the applicable rules of procedure.
3. The date by which the defendant may request additional discovery is extended pending review of the voluminous materials produced by the government to date.
4. A protective order has been entered by the Court in this case.
5. The date for filing discovery and/or dispositive motions shall be set at the next status conference.
6. By agreement of the parties, the government will make its initial expert disclosures 11 weeks before trial. The defense will make its expert disclosures 8 weeks before trial. The government may then make an additional expert disclosure 5 weeks before trial if additional expert(s) are needed to address matters raised in the defense disclosures.

7. The defenses of insanity, public authority and alibi have not been raised in this case.
8. This court finds and concludes, pursuant to the provisions of 18 U.S.C. § 3161(h)(7)(A) and Section 5(b)(7)(B) of the Plan for Prompt Disposition of Criminal Cases in the United States District Court for the District of Massachusetts (Statement of Time Limits Adopted by the Court and Procedures for Implementing Them, Effective December 2008) that the defendant requires additional time for the preparation of an effective defense, including time for review of the evidence, preparation of motions, and consideration of alternatives concerning how best to proceed with this matter, and that the interests of justice outweighs the best interests of the public and the defendant for a trial within seventy days of the return of an indictment.

Accordingly, it is hereby ordered that the Clerk of this Court enter excludable time for the period of March 1, 2012 through May 17, 2012, that being the period between the expiration of the last order on excludable time and the next status conference.

Based upon the prior orders of the court dated July 19, 2011, September 9, 2011, November 8, 2011, December 14, 2011, January 18, 2012, and the order entered contemporaneously herewith, at the time of the Interim Status Conference on May 17, 2012 there will be zero (0) days of non-excludable time under the Speedy Trial Act and seventy (70) days will remain under the Speedy Trial Act in which this case must be tried.

9. The parties believe that a trial is likely and that the trial will last approximately 3 weeks.
10. **An Interim Status Conference has been scheduled for May 17, 2012 at 2:30 p.m. Counsel for the respective parties shall file a Joint Memorandum addressing the matters set forth in LR 116.5(b) before the close of business no less than THREE business days prior to that Status Conference.**

/ s / Judith Gail Dein  
JUDITH GAIL DEIN  
UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

CRIMINAL No.  
11-10260-NMG

UNITED STATES OF AMERICA

v.

AARON SWARTZ

**ORDER ON EXCLUDABLE TIME**

March 16, 2012

DEIN, M.J.

With the agreement of the parties, this court finds and concludes, pursuant to the provisions of 18 U.S.C. § 3161(h)(7)(A) and Section 5(b)(7)(B) of the Plan for Prompt Disposition of Criminal Cases in the United States District Court for the District of Massachusetts (Statement of Time Limits Adopted by the Court and Procedures for Implementing Them, Effective December 2008) that the defendant requires additional time for the preparation of an effective defense, including time for review of the evidence, preparation of motions and consideration of alternatives concerning how best to proceed, and that the interests of justice outweighs the best interests of the public and the defendant for a trial within seventy days of the return of an indictment, and that not granting this continuance would deny counsel for the defendant a reasonable time necessary for effective preparation. See 18 U.S.C. § 3161(h)(7)(B)(iv).

Accordingly, it is hereby ordered that the Clerk of this Court enter excludable time for the period of

March 1, 2012 through May 17, 2012,

that being the period between the expiration of the last order on excludable time and the

next status conference.

Based upon the prior orders of the court dated July 19, 2011, September 9, 2011, November 8, 2011, December 14, 2011, January 18, 2012 and this order, at the time of the Interim Status Conference on May 17, 2012 there will be zero (0) days of non-excludable time under the Speedy Trial Act and seventy (70) days will remain under the Speedy Trial Act in which this case must be tried.

/ s / Judith Gail Dein  
JUDITH GAIL DEIN  
United States Magistrate Judge

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4307338@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Set/Reset Hearings  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 3/19/2012 at 3:47 PM EDT and filed on 3/19/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** No document attached

**Docket Text:**

**Set/Reset Hearings as to Aaron Swartz Status Conference set for 5/17/2012 02:30 PM in Courtroom 15 before Magistrate Judge Judith G. Dein. (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4363654@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Notice of Rescheduling  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 4/27/2012 at 10:13 AM EDT and filed on 4/27/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** No document attached

**Docket Text:**

**ELECTRONIC NOTICE OF RESCHEDULING from 5/17/12 to 5/22/12 from as to Aaron Swartz  
Status Conference set for 5/22/2012 02:30 PM in Courtroom 15 before Magistrate Judge  
Judith G. Dein. (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**



UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 11-10260-NMG
	)	
AARON SWARTZ,	)	
	)	
Defendant	)	

**JOINT MEMORANDUM IN ANTICIPATION OF INTERIM STATUS CONFERENCE**

The Court has scheduled the next Status Conference in this case for May 22, 2012. The parties will jointly request that the Court schedule a final status conference in 60 days i.e., during the week of July 23, 2012. This period is necessary for the defense to file discovery motions and the government to respond to such motions given that voluntary discovery is complete and the parties have substantially narrowed their disagreements regarding the proper scope of discovery such that judicial decision-making will be requested and required.

The parties request that the Court enter an amended order of excludable delay, correcting the Order dated March 19, 2012, Docket # 36. As reflected in paragraph 8 of the Court's March 16, 2012 Interim Status Report (Docket #35), the order of excludable delay was intended to cover the period through May 17, 2012 (when the next status conference was scheduled), rather than through April 2.

The parties further request that the Court enter an order of excludable delay under the Speedy Trial Act from May 17, 2012 to the date set by the Court for the Final Status Conference, on the grounds that the defendant intends to file timely motions, the Government requires additional time to respond, the parties have narrowed but not extinguished their differences

regarding the scope of discovery, and that the interests of justice outweighs the best interests of the public and the defendant for a trial within seventy days of the return of an indictment.

(1) The government has produced automatic discovery. In addition, the government has provided additional early discovery of many of the materials set forth in Local Rule 116.2(B)(2) and the Jencks Act in the form of a searchable electronic Concordance database.

(2) Additional discovery will be produced in accordance with the schedule established by the Local Rules of this Court, the Federal Rules of Criminal Procedure and by statute.

(3) The parties believe that early discovery provided by the government will enable the defense to better assess the case and any potential dispositive motions to be filed in it and will enable the parties to brief any contested matters for the Court with greater clarity. However, the defense reserved the right to make any additional discovery requests that are appropriate after review of the materials it has received from the government. The defense and government have narrowed the issues but not eliminated their differences on the proper scope of discovery. Discovery motions filed pursuant to the Local Rule protocol will be prepared and filed pursuant to a schedule set by the Court during the scheduled Interim Status Conference.

(4) A protective order has been entered by the Court in this case.

(5) There are no pending pretrial motions under Fed. R. Crim. P. 12(b). The parties request that the Court defer setting a schedule for the filing of dispositive motions in this case until the Final Status Conference in order to give the defense a sufficient opportunity to review any additional discovery it receives as a result of the discovery motions.

(6) The parties propose that expert witness disclosure in this case take place in three phases. The government will make its initial expert witness disclosure 11 weeks before trial.

The defense will make theirs 8 weeks before trial. The government may then make an additional expert disclosure 5 weeks before trial, if an additional expert or experts are necessary to address matters raised in the defense disclosure.

(7) The defenses of insanity, public authority and alibi have not been raised in this case.

(8) The Court should exclude the period from May 17, 2012 through the date of the next Interim Status Conference under the Speedy Trial Act.

(9) The parties believe that trial is likely and that the trial will last around 3 weeks.

(10) The parties request that the Final Status Conference be set for the week of July 23, 2012, in approximately 60 days.

Respectfully submitted,

Carmen M. Ortiz  
United States Attorney

Martin G. Weinberg  
MARTIN G. WEINBERG, Esq.  
Counsel for Defendant Aaron Swartz

By: Stephen P. Heymann  
STEPHEN P. HEYMANN  
SCOTT L. GARLAND  
Assistant U.S. Attorneys

#### CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

Stephen P. Heymann  
STEPHEN P. HEYMANN  
Assistant United States Attorney

Date: May 16, 2012

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4400331@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Status Conference by Magistrate Judge  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 5/22/2012 at 4:17 PM EDT and filed on 5/22/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** No document attached

**Docket Text:**

**ELECTRONIC Clerk's Notes for proceedings held before Magistrate Judge Judith G. Dein: Status Conference as to Aaron Swartz held on 5/22/2012; Counsel report discovery is ongoing and seek further conference for 7/26/12 @ 2:30pm.(Attorneys present: Heymann and Weinberg. )Court Reporter Name and Contact or digital recording information: Digital Recording – for transcripts or CDs contact Deborah Scalfani (deborah\_scalfani@mad.uscourts.gov). (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

CRIMINAL No.  
11-10260-NMG

UNITED STATES OF AMERICA  
v.

AARON SWARTZ

**INTERIM STATUS REPORT**

May 23, 2012

DEIN, M.J.

An Interim Status Conference, originally scheduled for May 17, 2012, was held before this court on May 22, 2012 pursuant to the provisions of Local Rule 116.5(b).

Based on that conference, this court enters the following report and orders, to wit:

1. The government has produced its automatic discovery as well as additional materials, and defendant is in the process of reviewing the materials produced by the government to date.
2. Any additional discovery will be produced in accordance with the applicable rules of procedure.
3. The parties have been working together to resolve their discovery disputes.
4. A protective order has been entered by the Court in this case.
5. The defendant shall file any discovery motions by **June 1, 2012**. The government shall respond by **June 22, 2012**.
6. By agreement of the parties, the government will make its initial expert disclosures 11 weeks before trial. The defense will make its expert disclosures 8 weeks before trial. The government may then make an additional expert disclosure 5 weeks before trial if additional expert(s) are needed to address matters raised in the defense disclosures.
7. The defenses of insanity, public authority and alibi have not been raised in this case.

8. This court finds and concludes, pursuant to the provisions of 18 U.S.C. § 3161(h)(7)(A) and Section 5(b)(7)(B) of the Plan for Prompt Disposition of Criminal Cases in the United States District Court for the District of Massachusetts (Statement of Time Limits Adopted by the Court and Procedures for Implementing Them, Effective December 2008) that the defendant requires additional time for the preparation of an effective defense, including time for review of the evidence, preparation of motions, and consideration of alternatives concerning how best to proceed with this matter, and that the interests of justice outweighs the best interests of the public and the defendant for a trial within seventy days of the return of an indictment.

Accordingly, it is hereby ordered that the Clerk of this Court enter excludable time for the period of May 17, 2012 through July 26, 2012, that being the period between the expiration of the last order on excludable time and the next status conference.

Based upon the prior orders of the court dated July 19, 2011, September 9, 2011, November 8, 2011, December 14, 2011, January 18, 2012, March 16, 2012 and the order entered contemporaneously herewith, at the time of the Final Status Conference on July 26, 2012 there will be zero (0) days of non-excludable time under the Speedy Trial Act and seventy (70) days will remain under the Speedy Trial Act in which this case must be tried.

9. The parties believe that a trial is likely and that the trial will last approximately 3 weeks.
10. **A Final Status Conference and hearing on any discovery motions has been scheduled for July 26, 2012 at 2:30 p.m. Counsel for the respective parties shall file a Joint Memorandum addressing the matters set forth in LR 116.5 before the close of business no less than THREE business days prior to that Status Conference.**

/ s / Judith Gail Dein  
JUDITH GAIL DEIN  
UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

CRIMINAL No.  
11-10260-NMG

UNITED STATES OF AMERICA

v.

AARON SWARTZ

**ORDER ON EXCLUDABLE TIME**

May 23, 2012

DEIN, M.J.

With the agreement of the parties, this court finds and concludes, pursuant to the provisions of 18 U.S.C. § 3161(h)(7)(A) and Section 5(b)(7)(B) of the Plan for Prompt Disposition of Criminal Cases in the United States District Court for the District of Massachusetts (Statement of Time Limits Adopted by the Court and Procedures for Implementing Them, Effective December 2008) that the defendant requires additional time for the preparation of an effective defense, including time for review of the evidence, preparation of motions and consideration of alternatives concerning how best to proceed, and that the interests of justice outweighs the best interests of the public and the defendant for a trial within seventy days of the return of an indictment, and that not granting this continuance would deny counsel for the defendant a reasonable time necessary for effective preparation. See 18 U.S.C. § 3161(h)(7)(B)(iv).

Accordingly, it is hereby ordered that the Clerk of this Court enter excludable time for the period of

May 17, 2012 through July 26, 2012,

that being the period between the expiration of the last order on excludable time and the next status conference.

Based upon the prior orders of the court dated July 19, 2011, September 9, 2011, November 8, 2011, December 14, 2011, January 18, 2012, March 16, 2012 and this order, at the time of the Final Status Conference on July 26, 2012 there will be zero (0) days of non-excludable time under the Speedy Trial Act and seventy (70) days will remain under the Speedy Trial Act in which this case must be tried.

/ s / Judith Gail Dein  
JUDITH GAIL DEIN  
United States Magistrate Judge



UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES	)	
	)	
v.	)	No. 11-10260-NMG
	)	
AARON SWARTZ	)	

**DEFENDANT AARON SWARTZ’S MOTION FOR DISCOVERY**

On May 8, 2012, defendant Aaron Swartz sought from the government 21 enumerated categories of discovery from the government. *See* Exhibit A, submitted herewith. That request was followed by a letter dated May 10, 2012, outlining the bases for the requests made in the earlier letter. *See* Exhibit B, submitted herewith. Following discussions by the parties conducted in good faith to eliminate and/or narrow the areas of dispute, the government responded to Swartz’s discovery requests on May 18, 2012. *See* Exhibit C, submitted herewith. This motion requests that the government be ordered to provide Swartz with the discovery which it has declined to produce: that described in paragraphs 1, 4, 6, 12, 15, and 20 of Swartz’s May 8, 2012, discovery request letter.

**I. PARAGRAPH 6.**

This paragraph requested that the government provide “[a]ny and all notes and reports provided to USSS or USAO by CERT in relation to their forensic analysis of the ACER laptop, or of any analysis of any other evidence including but not limited to the PCAP log information sent to CERT by the USSS for analysis.” “CERT” in this request refers to the Carnegie Mellon computer response team which provides assistance to the USSS with complex computer and internet issues.

In this case, CERT conducted analyses, which it provided to the United States Attorney's Office, of MIT computer/internet information relating to Swartz's alleged use of the MIT system and/or of certain computers or hard drives which the government associates with Swartz. Information received in discovery indicates that the flow traffic on MIT's network was being contemporaneously uploaded to the CERT "dropbox." The government has declined to provide these reports and other information on the ground that no CERT personnel will be appearing as expert witnesses at the trial of this case and that, if they do, such discovery should be subject to the separate schedule for the disclosure of reports of experts rather than to the obligations relating to disclosure of scientific results or tests. That fact, however, does not eliminate the defendant's entitlement to this information. Swartz is entitled to the production of reports of scientific tests under Fed. R. Evid. 16(a)(1)(F), which entitles the defendant to the "results or reports" of "any scientific test or experiment" if the item is in the possession of the government – as it is here – and if the item is material to the preparation of the defense *or* the government intends to use the item in its case-in-chief at trial. Rule 16(a)(1)(F) encompasses forensic examination of computer/internet data or information. *See, e.g., United States v. Pires*, 2009 WL 2176664 at \*1 (D.Mass. July 22, 2009); *United States v. Robinson*, 2006 WL 468298 at \*4 (N.D.Tex. Feb. 28, 2006). Here, the requested information is material to the preparation of Swartz's defense and to Swartz's potential ability to file a particularized motion to suppress asserting violations of 18 U.S.C. §2510 *et seq.* and/or the Fourth Amendment.

## **II. PARAGRAPH 12.**

This paragraph requested that the government provide:

As to the ACER laptop: the dates of any searches (defined as any attempt to see any information contained on the computer that would not be visible without touching the computer in any way including but not limited to any port scan of the computer, any imaging

of the laptop or any portion of its contents, any powering or opening of any file or folder or data contained in the laptop, any touching of a key or moving of a mouse so as to put in view new information, and any analysis or review by CERT or USSS of any of the contents of the laptop whether obtained remotely, by a physical search, or by a search of an image of the laptop), the identity of each individual who conducted any search of the laptop computer, the date of such search and the legal basis for each such search.

The government has provided Swartz with the February, 2011, search warrant authorizing the search of an ACER laptop alleged to have been used by Swartz in relation to the events which are the subject of the indictment in this case. However, Swartz has information indicating that the government attempted to gain access to the contents of the laptop and/or to modify the condition of the ACER laptop on January 6, 2011, the date of its seizure, and possibly at other times prior to the execution of the search warrant. Moving a mouse or touching a key on a computer which reveals information that was not in plain view constitutes a search which may not be lawfully conducted under the Fourth Amendment in the absence of a valid warrant. *See, e.g., United States v. Musgrove*, 2011 WL 4356515 at \*15 (E.D.Wis. September 16, 2011); *see also Arizona v. Hicks*, 480 U.S. 321 (1987). The requested information is critical to Swartz's ability to prepare a particularized motion to suppress unlawfully obtained evidence or other information if such incursions or attempted incursions into the contents of the laptop were made in the absence of a validly issued search warrant.

### **III. PARAGRAPH 15.**

This paragraph asked the government to "identify the origin of any and all statements of Aaron Swartz including but not limited to emails, text messages, chats, documents, memoranda or letters, i.e., to identify the source from which each statement was received and the legal procedure used to obtain each such statement of the defendant." Swartz has received in discovery internet

memoranda and chats purporting to be from him. For example, the discovery contains a number of chats on googlegroups.com which contain entries which facially indicate that Swartz was a participant in the communications. The discovery also contains a number of emails which on their faces indicate that they were either to or from Swartz. Swartz requires the additional information requested – the source of these statements and the procedure used by the government to obtain them – to enable him to move to suppress such statements if grounds exist to do so, which he cannot determine without the requested information. *See* Fed. R. Crim. P. 12(b)(4).

#### **IV. PARAGRAPHS 1, 4, 20.**

These paragraphs request information relating to grand jury subpoenas. Paragraph 1 requested that the government provide “[a]ny and all grand jury subpoenas – and any and all information resulting from their service – seeking information from third parties including but not limited to Twitter, MIT, JSTOR, Internet Archive that would constitute a communication from or to Aaron Swartz or any computer associated with him.” Paragraph 4 requested “[a]ny and all SCA applications, orders or subpoenas to MIT, JSTOR, Twitter, Google, Amazon, Internet Archive or any other entity seeking information regarding Aaron Swartz, any account associated with Swartz, or any information regarding communications to and from Swartz and any and all information resulting from their service.” Paragraph 20 requested “[a]ny and all paper, documents, materials, information and data of any kind received by the Government as a result of the service of any grand jury subpoena on any person or entity relating to this investigation.”

Swartz requests this information because some grand jury subpoenas used in this case contained directives to the recipients which Swartz contends were in conflict with Rule 6(e)(2)(A), *see United States v. Kramer*, 864 F.2d 99, 101 (11th Cir. 1988), and others sought certification of

the produced documents so that they could be offered into evidence under Fed. R. Evid. 803(6), 901. Swartz requires the requested materials to determine whether there is a further basis for moving to exclude evidence under the Fourth Amendment (even though the SCA has no independent suppression remedy).

The Fourth Amendment “provides protection against a grand jury subpoena too sweeping in its terms “to be regarded as reasonable.”” *United States v. Dionisio*, 410 U.S. 1, 11 (1973), *quoting Hale v. Henkel*, 201 U.S. 43, 76 (1906). *See United States v. Calandra*, 414 U.S. 338, 346 (1974)(“A grand jury’s subpoena duces tecum will be disallowed if it is ‘far too sweeping in its terms to be regarded as reasonable’ under the Fourth Amendment”); *In re Horowitz*, 482 F.2d 72, 79 (2d Cir. 1973)(“the Constitution undoubtedly protects against overly broad *subpoenas duces tecum*”); *In re Eight Grand Jury Subpoenae Duces Tecum*, 701 F.Supp. 53, 55 (S.D.N.Y. 1988)(grand jury “may not issue a subpoena so broad as to impinge unreasonably on legitimate fourth amendment rights”); *In re Grand Jury Subpoenas Served Feb. 27, 1984*, 599 F.Supp. 1006, 1017 (E.D. Wash. 1984)(“There is no doubt that a grand jury subpoena *duces tecum* must pass constitutional muster”). Swartz retains a reasonable expectation of privacy in his emails and chat communications even though they are in the hands of a third party internet service provider. *See United States v. Warshak*, 631 F.3d 266, 283-87 (2010).

Moreover, defendant believes that the items would not have been subpoenaed by the experienced and respected senior prosecutor, nor would evidentiary certifications have been requested, were the subpoenaed items not material to either the prosecution or the defense. Defendant’s viewing of any undisclosed subpoenaed materials would not be burdensome, and disclosure of the subpoenas would not intrude upon the government’s work product privilege, as the

subpoenas were served on third parties, thus waiving any confidentiality or privilege protections.

Respectfully submitted,  
By his attorney,

**/s/ Martin G. Weinberg**  
Martin G. Weinberg  
20 Park Plaza, Suite 1000  
Boston, MA 02116  
(617) 227-3700 (tel.)  
(617) 338-9538 (fax)  
owlmgw@att.net

#### **CERTIFICATE OF SERVICE**

I, Martin G. Weinberg, hereby certify that on this 1st day of June, 2012, a copy of the foregoing document has been served via the Court's ECF system on all registered participants, including Stephen P. Heymann, AUSA.

**/s/ Martin G. Weinberg**  
Martin G. Weinberg

Swartz  
Carr

**MARTIN G. WEINBERG, P.C.**  
**ATTORNEY AT LAW**

20 PARK PLAZA, SUITE 1000  
BOSTON, MASSACHUSETTS 02116

(617) 227-3700

FAX (617) 338-9538

NIGHT EMERGENCY:  
(617) 901-3472

EMAIL ADDRESSES:

owlmcb@att.net  
owlmgw@att.net

May 8, 2012

Stephen Heymann  
Assistant United States Attorney  
United States Attorney's Office  
1 Courthouse Way  
Boston, MA

RE: United States v. Aaron Swartz

Dear Mr. Heymann:

This letter is authored to request that you provide me with the following discovery that is material to the preparation of the above-captioned matter:

1. Any and all grand jury subpoenas – and any and all information resulting from their service - seeking information from third parties including but not limited to Twitter, MIT, JSTOR, Internet Archive that would constitute a communication from or to Aaron Swartz or any computer associated with him;
2. Any and all grand jury subpoenas – and any and all information resulting from their service - seeking information regarding the defendant wherein the receiver of the subpoena is warned that disclosure to third parties would or could or might impede the investigation or containing any indirect or direct references that disclosure might impede or obstruct a criminal investigation;
3. Any and all grand jury subpoenas – and any and all information resulting from their services – which contain a request for a certificate of authenticity and/or a certificate wherein a record keeper or representative of the entity receiving the subpoena affirms information about the produced records that would meet either hearsay or authenticity evidentiary challenges;
4. Any and all SCA applications, orders, or subpoenas to MIT, JSTOR, Twitter, Google, Amazon, Internet Archive, or any other entity seeking information regarding



Aaron Swartz, any account associated with Swartz, or any information regarding communications to and from Swartz and any and all information resulting from their service;

5. Any and all preservation letters sent to MIT in relation to this investigation that require that MIT preserve the results of all recorded or captured router data resulting from MITs utilization of programs or hardware to create tcpdump formatted files beginning no later than 11-7-2010;

6. Any and all notes and reports provided to USSS or USAO by CERT in relation to their forensic analysis of the ACER laptop, or of any analysis of any other evidence including but not limited to the PCAP log information sent to CERT by the USSS for analysis;

7. Any and all fingerprint reports comparing the known prints of Aaron Swartz or any other person with any latent or unknown prints lifted from any evidence in relation to this case (other than such reports that were already disclosed);

8. Any and all telephone toll records subpoenaed or otherwise obtained in relation to this case;

9. Any and all credit card statements or account information subpoenaed or otherwise obtained in relation to this case;

10. Any and all documents reflecting the purchase of computers or computer software or external hard-drives that are material to this case;

11. Any and all Grand Jury testimony provided on or about 6-16-11 and any memoranda of interview of Quinn Norton;

12. As to the ACER laptop: the dates of any searches (defined as any attempt to see any information contained on the computer that would not be visible without touching the computer in anyway including but not limited to any port scan of the computer, any imaging of the laptop or any portion of its contents, any powering or opening of any file or folder or data contained in the laptop, any touching of a key or moving of a mouse so as to put into view new information, and any analysis of review by CERT or USSS of any of the contents of the laptop whether obtained remotely, by a physical search, or by a search of an image of the laptop), the identity of each individual who conducted any search of the laptop computer, the date of such search and the legal basis for each such search;

13. As to any evidence seized from the backpack of the defendant on January 6, 2011, the same requests as in paragraph 12, supra;

14. Any and all chain of custody reports from USSS and other federal entities regarding any intended government exhibit;

15. To identify the origin of any and all statements of Aaron Swartz including but not limited to emails, text messages, chats, documents, memoranda or letters ie. to identify



the source from which each such statement was received and the legal procedure used to obtain each such statement of the defendant as required by FRCrimP 12(d)(1);

16. Any and all information including but not limited to 70 gigabytes or more of historical network flow data dating from 12-14-10 through 1-6-11 and all DHCP log information provided to S/A Pickett by MIT employees including but not limited to Michael Halsall (see log pg 7) to the extent that such flow data, radius logs, network capture data and DHCP log information was not provided to the defendant on or about November 18, 2011;

17. Any and all additional (a) IP connection logs and/or DHCP logs, (b) radius logs, (c) flow data files, and (d) network capture files that the USSS or any other federal entity received from MIT or JSTOR (some but not all of such logs were provided to the defense and this request is for any other such logs, network capture files, or flow data that was received from MIT or JSTOR in connection to this investigation regardless of whether it was associated with IP addresses alleged to have been used by the defendant);

18. Any and all additional documents, reports, data, or other information received from MIT or JSTOR that is outside paragraphs 16 and 17 and not previously provided to the defendant in discovery and the legal vehicle if any which resulted in the transmission of such information to the Government;

19. As to any MAC addresses that the Government associates with the defendant, when was information about each received, from who, pursuant to what process;

20. Any and all paper, documents, materials, information, and data of any kind received by the Government as a result of the service of any grand jury subpoena on any person or entity relating to this investigation; and

21. Any and all paper, documents, materials, information and data of any kind received by the Government from the Middlesex District Attorney or any state or city law enforcement authority that resulted from the service of any state grand jury subpoena on any person or entity relating to this investigation

If you believe that you have already provided me with the entirety of the materials requested in any paragraph, please so inform me. If you believe that you have provided me with some but not all of the requested information, please provide the remainder. If you want to discuss the basis for these requests, beyond the requirements of Rule 16 and corresponding Local Rules, please advise as to which paragraphs.

Yours Truly,

Martin G. Weinberg, Esq.

**MARTIN G. WEINBERG, P.C.**  
**ATTORNEY AT LAW**

20 PARK PLAZA, SUITE 1000  
BOSTON, MASSACHUSETTS 02116

(617) 227-3700

FAX (617) 338-9538

NIGHT EMERGENCY:  
(617) 901-3472

EMAIL ADDRESSES:

owlmcb@att.net  
owlmgw@att.net

May 10, 2012

Stephen Heymann  
Assistant United States Attorney  
United States Attorney's Office  
1 Courthouse Way  
Boston, MA

RE: *United States v. Aaron Swartz*

Dear Mr. Heymann:

You have requested that I supplement my letter to you dated May 8, 2012, by disclosing the legal basis for my requests contained therein.

1. As to paragraphs 1, 2, 3, 8, 9, 10, 18, 20, and 21, the objective is to discover information and inspect papers and documents within the Government's possession that are material to preparing the defense in this case, see Fed. R. Crim. P. 16(a)(1)(E)(i). The presupposition for each paragraph is that I am seeking documentary evidence that you subpoenaed or otherwise acquired from third parties in relation to this investigation. Given that you would not issue overbroad subpoenas, I would assume that what you were provided was material to the investigation and hence to the defense for this matter. As to paragraph 1, I am also seeking information pursuant to Rule 16(a)(1)(A) and, to the extent you received emails or other communications of the defendant that were stored for him by a third party, I rely on Rule 16(a)(1)(E)(iii). As to paragraph 2, I believe full discovery is the minimal response to the inappropriate threat that is on the face of at least one of your grand jury subpoenas. See, e.g. *United States v. Kramer* 864 F.2d 99, (11<sup>th</sup> cir. 1988). As to paragraph 3, I rely upon Rule 16(a)(1)(E)(i),(ii).

2. As to paragraphs 4, 5, 12, 13, 14, 16, 17, and 19, I rely on Rule 16(a)(1)(E)(i),(iii) and in particular on the relationship between such requested discovery and Mr. Swartz' rights to protect his Fourth Amendment and Title III rights in this case. I also invoke Fed. R. Crim. P. 12(b)(4): although the rule is literally confined to evidence you intend to

use (I would request that you make this disclosure), I would need as well to determine if the February, 2011, court authorized searches were tainted by the January, 2011, warrantless searches.

3. As to paragraph 11, *Brady v. Maryland*, 373 U.S. 83 (1963).
4. As to paragraph 15, Rule 16(a)(1)(B).
5. As to paragraphs 6 and 7, Rule 16(a)(1)(F).

I think a paragraph by paragraph review of the requests and your proposed responses prior to our need to draft a status conference report for May 22, 2012, makes sense.

Thanks,

Martin G Weinberg, Esq.





**U.S. Department of Justice**

***Carmen M. Ortiz***  
*United States Attorney*  
*District of Massachusetts*

---

*Main Reception: (617) 748-3100*

*John Joseph Moakley United States Courthouse*  
*1 Courthouse Way*  
*Suite 9200*  
*Boston, Massachusetts 02210*

May 18, 2012

Martin G. Weinberg  
20 Park Plaza  
Suite 1000  
Boston, MA 02116

Re: U.S. v. Aaron Swartz

Dear Mr. Weinberg:

This letter formalizes in accordance with Local Rule 116.3(a) my response to your letter request for additional discovery dated May 8, 2012. I found our lengthy discussions on Tuesday concerning your various requests very helpful in identifying and narrowing those areas in which we have meaningful disagreements that will need to be considered and resolved by the court.

We have previously provided to you and your predecessor counsel not only all material described in Federal Rule of Criminal Procedure 16 and Local Rules 116.1 and 116.2 as being appropriate at this stage of the criminal case, but also an extensive body of email, computer logs, law enforcement reports, photographs and video recordings created and concerning the events and investigation leading to your client's arrest in the organized form of a Concordance database. Except as set forth below, we cannot agree to furnish the materials which you have requested to the extent that they go beyond the very large body of materials which we have already produced which already far exceed those required by the local and federal rules, and the statutes and constitutional provisions they embody. We cannot see how many of the materials you have requested are material to the defense and many others, as we discussed, are either privileged or will be furnished at later times as specified by the Court, rules and governing statutes.

In light of our useful discussions, and again in the hope of narrowing those potential discovery disputes which the court will need to resolve, this letter will also serve to confirm the following aspects of our discussions:

1. A central focus of our discussions were suppression remedies you potentially thought you might pursue. As you are aware, there is no suppression remedy under the Stored Communications Act. *See* 18 U.S.C. § 2708. To the extent that you believe it was necessary to

Martin G. Weinberg

May 18, 2012

Page 2

obtain a warrant under Rule 41 of the Federal Rules of Criminal Procedure or 18 U.S.C. §2703 before conducting a particular search, copies of all warrants obtained during the investigation of this case were provided to your predecessor counsel on August 12, 2011. I understand that all of these were transferred to you when you took over the case, but, if not, please do not hesitate to let me know and I will forward a second set to you.

2. You previously have been provided with all MIT logging data in the government's possession pertaining to your client relevant to this case. The government received from MIT additional RADIUS logs which the government has been informed pertain only to third parties who happened to have plugged into MIT's computer network on January 6, 2011 as well. Based on your representation that the third-party logging information is material to the defense of this case, the government has no objection to providing to you the additional logs, subject to paragraph 2(a)(v)(b) of the Protective Order entered in this case.

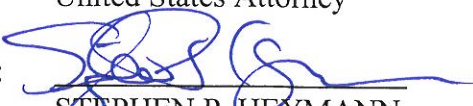
3. You have previously been provided all reports of fingerprint examinations conducted during the federal investigation of this case.

4. In keeping with Local Rule 116.8, we have sought to obtain any information subject to disclosure from all federal, state and local law enforcement agencies formally participating in the criminal investigation that resulted in this case.

Yours very truly,

CARMEN M. ORTIZ  
United States Attorney

By:

  
STEPHEN P. HEYMANN  
Assistant U.S. Attorney

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 11-10260-NMG
	)	
AARON SWARTZ,	)	
	)	
Defendant	)	

Government's Response to Defendant Aaron Swartz's Motion for Discovery

The government has provided extensive discovery in this case, voluntarily going well beyond the requirements of Federal Rule of Criminal Procedure 16, the Local Rules and the Constitution in order to give the defendant and his counsel a clear view of the investigation that preceded the defendant's arrest. The defendant has responded with four very broad discovery requests effectively seeking access to the entirety of the government's investigative files and work product. These requests should be denied. The Supreme Court has explicitly "rejected the notion that a 'prosecutor has a constitutional duty routinely to deliver his entire file to defense counsel.'" *Arizona v. Youngblood*, 486 U.S. 51, 55 (1988) (quoting *United States v. Agurs*, 427 U.S. 97, 111 (1976)). *See also Moore v. Illinois*, 488 U.S. 786, 795 (1972) ("We knew of no constitutional requirement that the prosecution make a complete and detailed accounting to the defense of all police investigatory work on a case.")

Background Common to Defendant's First Two Requests

The Indictment charges that:

Between September 24, 2010 and January 6, 2011, Swartz contrived to:

- a. break into a computer wiring closet at MIT;
- b. access MIT's network without authorization from a switch within that closet;

- c. connect to JSTOR's archive of digitized journal articles through MIT's computer network;
- d. use this access to download a major portion of JSTOR's archive onto his computers and computer hard drives;
- e. avoid MIT's and JSTOR's efforts to prevent this massive copying, measures which were directed at users generally and Swartz's illicit conduct specifically; and
- f. elude detection and identification;

all with the purpose of distributing a significant portion of JSTOR's archive through one or more file-sharing sites.

Indictment (Docket #2) at ¶ 11.

Swartz used an ACER laptop, among other equipment, to access MIT's computer network and to steal JSTOR's files. Having searched for the source of the illegal JSTOR downloads for months, MIT finally located the laptop on January 4, 2010, in a restricted wiring closet in the basement of an MIT building hidden under a box and hard-wired into a computer switch. MIT contacted local and federal law enforcement officers and began monitoring what the then-unidentified hacker's computer was doing on their network. The computer logs of these activities were subsequently provided to the United States Secret Service.

When called in, law enforcement officers photographed the scene and lifted fingerprint impressions from the computer. They also examined the computer itself and determined it was password protected, prohibiting them from taking forensic steps only possible before a computer is turned off.

Swartz was identified as the unknown hacker and thief after he was videotaped returning to the closet twice, on one occasion trying to shield his identity by holding a bicycle helmet over

his face. On the second occasion, he moved the ACER laptop from the restricted basement wiring closet to another location at MIT, where it was ultimately recovered by law enforcement officers. Swartz was arrested a short time later after fleeing police.

I. Paragraph 6<sup>1</sup>

The defendant has requested first that the government provide “[a]ny and all notes and reports provided to USSS or USAO by CERT in relation to the forensic analysis of the ACER laptop, or any analysis of any evidence including but not limited to the PCAP log information sent to CERT by the USSS for analysis.” The Court should deny this request because it seeks expert opinions long in advance of the schedule previously agreed upon by the parties and ordered by the Court, and also because it seeks materials covered by the work product privilege.

The United States Secret Service obtained a warrant to search the laptop, and then performed a forensic examination of the computer. To obtain expert opinions of both the contents of the laptop and the logs of its activities on MIT’s network, the Secret Service turned to CERT. CERT is Carnegie Mellon University’s Computer Emergency Response Team, which assists the Secret Service with complex computer matters. CERT identified files from the laptop’s hard drive that it considered potentially material to the prosecution of this case. It also provided preliminary opinions about how to interpret software code found on the laptop.<sup>2</sup>

The government has not determined who it will call as an expert at trial. Nor has the government asked any expert to prepare a final expert report concerning the contents of the

---

<sup>1</sup> For clarity, the government refers to the defendant’s requests using the same subheadings used in the Defendant’s motion.

<sup>2</sup> A similar investigative pattern was followed with respect to a number of hard drives and a USB drive seized during the investigation.



laptop or anything else.

CERT's margin descriptions and other preliminary interpretations of software and files on the seized laptop computer are not discoverable. *See United States v. Iglesias*, 881 F.2d 1519, 1523 (9<sup>th</sup> Cir. 1989) (holding that government satisfied its obligation to produce results and reports under Fed. R. Crim. P. 16 by turning over lab report determining substance to be 54.9% heroin and was not required to contemporaneously turn over log notes, protocols, and other internal documents of chemist because they did not have the requisite formality or finality to be considered as either a "report" or "result"); *United States v. Wilkerson*, 189 F.R.D. 14, 15-16 (D.Ma. 1999) (Collings, J.) (holding that records, notes and documentation concerning drug testing of controlled substance were not results or reports of test under Rule 16). Fed. R. Crim. P. 16 (a)(2) expressly states that the rule, "does not authorize the discovery or inspection of reports, memoranda, or other internal documents made by an attorney for the government or other government agent in connection with investigating or prosecuting the case."

Even were the margin descriptions and preliminary interpretations sufficiently formal or final to be considered "reports" or "results," they are not discoverable at this particular time. In *U.S. v. Pires*, 2009 WL 2176664 (D. Mass. July 22, 2009), relied on by the defendant, Judge Zobel ruled on two separate arguments by a defendant that he should be provided the results of the examination of his computer's contents during discovery. She required the government to describe substantively the *contents* of evidence found on a computer on which it intended to rely pursuant to Rule 16(a)(1)(F) (reports of examinations), which is timed earlier in the discovery process. Then she obligated the government to produce *interpretations* of and *inferences* from that evidence which it intended to elicit from its experts pursuant to Rule 16(a)(1)(G) (expert

opinions), which is timed later in the process.

The government has previously provided the defendant a complete copy of the ACER laptop's hard drive and a forensic report of its examination. It does not object, in light of *Pires*, to early identification of files, records and software code which it has determined to date may be material and offered as evidence at trial. In keeping with the distinction drawn in *Pires*, this Court should deny the defendant's motion to the extent that it seeks any opinions drawn about the meaning of that source code provided to the U.S. Attorney's Office or the United States Secret Service by CERT. To do otherwise, would provide raw investigative work product to the defendant. It also would completely undermine the schedule of expert disclosure explicitly agreed upon by the parties, submitted by them jointly to the Court, and directed in the Interim Status Reports. *See, e.g.*, Interim Status Report, May 23, 2012 (Docket # 38) at ¶ 6.

## II. Paragraph 12

In his next request, the defendant seeks the dates and identities of each person who ever touched the ACER laptop and a written legal justification for that person doing so. The defendant's request should be denied. The government not only has fully complied with its obligations under Local Rule 116.1(c)(1)(B) concerning the production of search materials, but also, well beyond that.

Local Rule 116.1(a)(1)(B) details the government's obligations in this district with respect to search materials. The government has greatly exceeded compliance with its discovery obligation with respect to searches. It has, of course, provided copies of all search warrants in this case. But, beyond that, it has provided the email traffic at MIT reflecting investigative steps being taken by them, all police and agent reports from the date of the ACER's discovery to its

seizure and the defendant's arrest, and even an internal U.S. Attorney's Office email containing facts concerning the handling of the ACER laptop upon its discovery which, upon initial review, government counsel did not see contained in other reports being provided to the defendant.

The defendant claims that additional discovery is necessary because even touching a computer key may be an unlawful search without a warrant. While he might be able to argue this extreme claim if the computer had been touched in defendant's apartment or office, he lost all reasonable expectation of privacy in the computer once he broke into MIT's wiring closet to steal JSTOR's files through MIT's hacked network and hid the computer under a box.

A trespasser who conceals personal items in someone else's property cannot assert the Fourth Amendment as a basis for challenging the search. *United States v. Terry*, 2001 WL 496630 at \*2, n.5 (S.D.Ga. 2007); *United States v. Pitt*, 717 F.2d 1334-37 (11<sup>th</sup> Cir. 1983) (holding defendant lacks standing where he was a trespasser "who assumed to lock the door which he had no legal right to lock"); *United States v. Sanchez*, 635 F.2d 47, 64 (2<sup>nd</sup> Cir. 1980) ("[A] mere trespasser has no Fourth Amendment protection in premises he occupies wrongfully."); *United States v. Hightower*, 1987 WL 44897 at \* 2 (6<sup>th</sup> Cir. Sept. 28, 1987) (holding that country club member who placed lock on a locker that he had not been assigned and on which he had not paid the annual rental fee "was in essence a trespasser" whose expectation of privacy was not legitimate); see 6 Wayne R. LaFare, Search and Seizure § 11.3(d), at 185 n.234 (4<sup>th</sup> ed. 2004) ("[A] trespasser certainly does not have standing"); *Rakas v. Illinois*, 439 U.S. 128, 143 (1987) ("Obviously, ... a 'legitimate' expectation of privacy by definition means more than a subjective expectation of not being discovered. A burglar plying his trade in a summer cabin during the off-season may have a thoroughly justified subjective

expectation of privacy, but it is not one which the law recognizes as ‘legitimate.’ His presence ... is ‘wrongful’; his expectation is not ‘one that society is prepared to recognize ‘reasonable.’”).

The defendant already has the facts and evidence to determine whether he has grounds to file a motion to suppress. Ordering that the government provide a written legal justification for steps taken by it during an investigation is outside the scope of pretrial discovery. The defendant’s request that the government prepare further documentation of the handling of his ACER laptop and its legal justification for doing so is wholly without merit and should be denied.

### III. Paragraph 15

In Paragraph 15, the defendant would require the government to identify the origin of any and all statements of Aaron Swartz in its possession and the legal procedure used to obtain the statements. All of the emails, text messages, chat sessions, and documents containing statements provided by the defendant relevant to this case were obtained either from individuals with whom the defendant communicated or from publicly available websites stored on the Internet. No emails, texts messages, chat logs, or documents were obtained from Internet service providers using orders under 18 U.S.C. 2703(d). As previously represented to defense counsel, there was no court-authorized electronic surveillance in this case.

The government objects to further particularization at this time. First, further particularization would identify witnesses long in advance of the time prescribed by the Local Rules. Second, as with his claim that he is entitled to an immediate written legal justification for each touching of his laptop, his demand for a written legal justification for each occasion during an investigation the government obtained a copy of something he wrote is outside the

scope of pretrial discovery.

#### IV. Paragraphs 1, 4, 20

Lastly, the defendant seeks any and all grand jury subpoenas and any and all information resulting from them, in essence, complete and open access to all aspects of the government's investigative files, including the statements of all witnesses before the grand jury and all documents and records obtained during the course of the investigation. Both Federal Rule of Criminal Procedure 16 and Local Rules 116.1-116.2 dispositively reject the concept of "open file" discovery in the federal courts. The defendant's request in this regard should be denied.

As a pre-requisite, the defendant has not established standing to move to suppress the subpoenas issued in the course of the grand jury investigation. "When those seeking to challenge a subpoena directed to a third party claim standing to raise a Fourth or Fifth Amendment issue, they must establish either the existence of a privileged relationship or of a legitimate property or privacy interest in the documents possessed by the third party." *In re Grand Jury Proceedings (Diamonte)*, 814 F.2d 61, 66 (1<sup>st</sup> Cir. 1987).

The defendant instead moves directly to three vague justifications for his request. First, he suggests that some unspecified grand jury subpoenas used in this case contained "*directives*" to the recipients in conflict with Rule 6(e)(2)(A), which states that "no obligation of secrecy may be imposed on any person except in accordance with Rule 6(e)(2)(B)." None of the subpoenas used in this case contained a "*directive*" to recipients of secrecy. Most were accompanied by a letter containing a *request* consistent with controlling First Circuit precedent, stating in pertinent part:

We request that you not disclose the existence of the subpoena, or the fact of your compliance with it, to anyone. *While you are not required to comply with this*

*request, any such disclosure could impede the investigation and interfere with the enforcement of federal criminal law.*

The First Circuit has expressly approved such requests and expressions of opinion: “The government is free to express its beliefs about the impact of any disclosure, provided it makes clear that the law does not require non-disclosure.” *In re Grand Jury Proceedings (Diamonte)*, 814 F.2d at 70.

Second, the defendant urges, without any factual evidence or basis, that some of the government’s grand jury subpoenas may have been “too sweeping in terms ‘to be regarded as reasonable.’” There is no basis for the defendant getting unprecedented access to all of the government’s grand jury subpoenas, grand jury transcripts, and documents and records produced by witnesses in response to those subpoenas based solely on the defendant’s bald conclusory assertion that some might have been overly broad.

Finally, with a coy use of the word “material,” the defendant argues that he is entitled to the entire investigative file because a senior prosecutor would not have sought the materials during an investigation were they not material to the prosecution or the defense. As complimentary as the apparent tautology may be, it fails in two, independent regards.

During an investigation, the government subpoenas records and obtains testimony before the grand jury that in good faith it prospectively believes may be relevant to the investigation. Not being omniscient, records and testimony often turn out not to be material to the prosecution or defense of the case as charged. They lead to investigative dead ends or the production of records or testimony which upon analysis turn out to be off point. Requiring the government to produce all of the government subpoenas, all grand jury testimony that followed, and all of the documents and records which were received would cause problems that the rules were designed

to prevent. It would result in disclosure of witnesses before the grand jury contrary to the specific intent of Fed. R. Crim. P. 6(e)(2), the transfer of records and documents to the defendant belonging to otherwise uninvolved third parties, and the disclosure of the work product and thought processes of the U.S. Attorney's Office during its investigation.

Furthermore, the request seeks to sidestep specific timing requirements created by statute and the local rules. For example while grand jury transcripts may be material both to the prosecution and the defense, the Jencks act and Local Rule 117.1(a)(5) reflect the determination that they need be provided only as trial approaches, and not before.

For these reasons, the defendant's over-reaching requests that he be provided all grand jury subpoenas and what was obtained pursuant to those subpoenas should be denied.<sup>3</sup>

Respectfully submitted,

Carmen M. Ortiz  
United States Attorney

By: /s/ Stephen P. Heymann  
STEPHEN P. HEYMANN  
SCOTT L. GARLAND  
Assistant U.S. Attorneys

Date: June 22, 2012

---

<sup>3</sup> As stated earlier, there were no applications pursuant to 18 U.S.C. §2703(d) for records from electronic communications service providers in this case. Accordingly, to the extent the defendant's request seeks these applications and orders, the defendant's request is moot.

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/s/ Stephen P. Heymann  
STEPHEN P. HEYMANN  
Assistant U. S. Attorney

Date: June 22, 2012



UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 11-10260-NMG
	)	
AARON SWARTZ,	)	
	)	
Defendant	)	

**JOINT MEMORANDUM AS TO FINAL STATUS CONFERENCE PURSUANT TO**  
**LOCAL RULE 116.5**

The Court has scheduled the final Status Conference in this case for July 26, 2012. The parties file this joint status report:

(1) The government has produced automatic discovery. In addition, the government has provided additional early discovery of many of the materials set forth in Local Rule 116.2(B)(2) and the Jencks Act in the form of a searchable electronic Concordance database.

(2) Additional discovery will be produced in accordance with the schedule established by the Local Rules of this Court, the Federal Rules of Criminal Procedure and by statute.

(3) A multi-request discovery motion filed pursuant to the Local Rule protocol was filed pursuant to a schedule set by the Court during the scheduled Interim Status Conference with decisions on contested matters pending with this Court.

(4) A protective order has been entered by the Court in this case.

(5) There are no pending pretrial motions under Fed. R. Crim. P. 12(b). The parties have requested that the Court defer setting a schedule for the filing of dispositive motions in this case until the Final Status Conference in order to give the defense a sufficient opportunity to review any

additional discovery it receives as a result of the discovery motions. The defense intends to file Motions to Suppress and Dismiss. The parties agree that such motions will be filed raise complex matters and that the Court should set a filing date for such matters 60 days from the date of the status conference;

(6) The parties propose that expert witness disclosure in this case take place in three phases. The government will make its initial expert witness disclosure 11 weeks before trial. The defense will make theirs 8 weeks before trial. The government may then make an additional expert disclosure 5 weeks before trial, if an additional expert or experts are necessary to address matters raised in the defense disclosure.

(7) The defenses of insanity, public authority and alibi have not been raised in this case.

(8) The Court should exclude the period from July 26, 2012 through the date of the next First Status Conference with the District Court under the Speedy Trial Act.

(9) The parties believe that trial is likely and that the trial will last around 3 weeks.

Respectfully submitted,

Carmen M. Ortiz  
United States Attorney

/s/ Martin G. Weinberg  
MARTIN G. WEINBERG, Esq.  
Counsel for Defendant Aaron Swartz

By: /s/ Stephen P. Heymann  
STEPHEN P. HEYMANN  
SCOTT L. GARLAND  
Assistant U.S. Attorneys

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the

registered participants as identified on the Notice of Electronic Filing (NEF).

/s/ Martin G. Weinberg  
Martin G. Weinberg  
Counsel for Defendant Aaron Swartz

Date: July 25, 2012

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4490144@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Status Conference by Magistrate Judge  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 7/27/2012 at 1:52 PM EDT and filed on 7/26/2012

**Case Name:** USA v. Swartz  
**Case Number:** 1:11-cr-10260-NMG  
**Filer:**  
**Document Number:** 43(No document attached)

**Docket Text:**

**ELECTRONIC Clerk's Notes for proceedings held before Magistrate Judge Judith G. Dein: Final Status Conference as to Aaron Swartz held on 7/26/2012, Motion Hearing as to Aaron Swartz held on 7/26/2012 re [40] MOTION for Discovery filed by Aaron Swartz; Counsel report current case status; USMJ Dein hears arguments on motion and takes motion under advisement. Court Reporter Name and Contact or digital recording information: Digital Recording – for transcripts or CDs contact Deborah Scalfani (deborah\_scalfani@mad.uscourts.gov). (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

CRIMINAL No.  
11-10260-NMG

UNITED STATES OF AMERICA  
v.

AARON SWARTZ

**FINAL STATUS REPORT**

August 1, 2012

DEIN, M.J.

A Final Status Conference and hearing on defendant's motion for discovery was held before this court on July 26, 2012 pursuant to the provisions of Local Rule 116.5(b). Based on that conference, this court enters the following report and orders, to wit:

1. The parties anticipate a trial in this matter.
2. This court has, on this date, issued an order on defendant's motion for discovery ordering the government to produce a limited amount of additional discovery by August 15, 2012.
3. There are no outstanding or anticipated discovery motions.
4. The defendant intends to file dispositive motions. The deadline for filing such motions is **September 28, 2012**. The government's response to such motions is due on **October 30, 2012**.
5. By agreement of the parties, the government will make its initial expert disclosures 11 weeks before trial. The defense will make its expert disclosures 8 weeks before trial. The government may then make an additional expert disclosure 5 weeks before trial if additional expert(s) are needed to address matters raised in the defense disclosures.
6. This court finds and concludes, pursuant to the provisions of 18 U.S.C. § 3161(h)(7)(A) and Section 5(b)(7)(B) of the Plan for Prompt Disposition of Criminal Cases in the United States District Court for the District of Massachusetts (Statement of Time Limits Adopted by the Court and

Procedures for Implementing Them, Effective December 2008) that the defendant requires additional time for the preparation of an effective defense, including time for review of the evidence, preparation of motions, and consideration of alternatives concerning how best to proceed with this matter, and that the interests of justice outweighs the best interests of the public and the defendant for a trial within seventy days of the return of an indictment.

Accordingly, it is hereby ordered that the Clerk of this Court enter excludable time for the period of July 26, 2012 through October 30, 2012, that being the period between the expiration of the last order on excludable time and the date by which the government must respond to the defendant's dispositive motions.

Based upon the prior orders of the court dated July 19, 2011, September 9, 2011, November 8, 2011, December 14, 2011, January 18, 2012, March 16, 2012, May 23, 2012 and the order entered contemporaneously herewith, as of October 30, 2012 there will be zero (**0**) days of non-excludable time under the Speedy Trial Act and seventy (**70**) days will remain under the Speedy Trial Act in which this case must be tried.

7. The parties believe that a trial is likely and that the trial will last approximately 3 weeks.
8. The file is hereby ordered returned to the District Judge to whom this case is assigned for further proceedings.

/ s / Judith Gail Dein  
JUDITH GAIL DEIN  
UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

CRIMINAL No.  
11-10260-NMG

UNITED STATES OF AMERICA

v.

AARON SWARTZ

**ORDER ON EXCLUDABLE TIME**

August 1, 2012

DEIN, M.J.

With the agreement of the parties, this court finds and concludes, pursuant to the provisions of 18 U.S.C. § 3161(h)(7)(A) and Section 5(b)(7)(B) of the Plan for Prompt Disposition of Criminal Cases in the United States District Court for the District of Massachusetts (Statement of Time Limits Adopted by the Court and Procedures for Implementing Them, Effective December 2008) that the defendant requires additional time for the preparation of an effective defense, including time for review of the evidence, preparation of motions and consideration of alternatives concerning how best to proceed, and that the interests of justice outweighs the best interests of the public and the defendant for a trial within seventy days of the return of an indictment, and that not granting this continuance would deny counsel for the defendant a reasonable time necessary for effective preparation. See 18 U.S.C. § 3161(h)(7)(B)(iv).

Accordingly, it is hereby ordered that the Clerk of this Court enter excludable time for the period of

July 26, 2012 through October 30, 2012,

that being the period between the expiration of the last order on excludable time and the date by which the government must respond to the defendant's dispositive motions.

Based upon the prior orders of the court dated July 19, 2011, September 9, 2011, November 8, 2011, December 14, 2011, January 18, 2012, March 16, 2012, May 23, 2012 and this order, as of October 30, 2012 there will be zero (0) days of non-excludable time under the Speedy Trial Act and seventy (70) days will remain under the Speedy Trial Act in which this case must be tried.

/ s / Judith Gail Dein  
JUDITH GAIL DEIN  
United States Magistrate Judge



UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

Criminal No.  
11-10260-NMG

UNITED STATES OF AMERICA

v.

AARON SWARTZ

**ORDER ON MOTION FOR DISCOVERY**

August 1, 2011

DEIN, M.J.

This matter is before the court on “Defendant Aaron Swartz’s Motion for Discovery” (Docket No. 40). After consideration of the pleadings and argument of counsel, the motion is ALLOWED IN PART and DENIED IN PART as follows:

1. **Paragraph 6:** By this request, the defendant is seeking notes and reports provided by CERT in connection with its forensic analysis of Swartz’s ACER laptop. The defendant relies on Fed. R. Crim. Pro. 16(a)(1)(F), which provides in relevant part that, upon request, “the government must permit a defendant to inspect and to copy or photograph the results or reports of any . . . scientific test or experiment if . . . (iii) the item is material to preparing the defense or the government intends to use the item in its case-in-chief at trial.” Swartz argues, without any details, that “the requested information is material to the preparation of Swartz’s defense and to Swartz’s potential ability to file a particularized motion to suppress asserting violations of 18 U.S.C. §

2510 *et seq.* and/or the Fourth Amendment.” (Mot. at 2). The government contends that the requested information is expert discovery, and that its disclosure is premature at this time.

This court agrees with the government that the reference in Rule 16(a)(1)(F) to “results or reports” does not include “CERT’s margin descriptions and other preliminary interpretations of software and files on the seized laptop” (Resp. at 4) that “do not have the requisite formality or finality to be considered as either a ‘report’ or a ‘result.’” United States v. Iglesias, 881 F.2d 1519, 1523 (9th Cir. 1989). This court also agrees that the disclosure of expert “interpretations and inferences from the evidence” is premature given the agreed-upon expert disclosure schedule. (See Resp. at 4). Nevertheless, the Rule is clear that the government is to produce the factual reports generated by CERT.<sup>1</sup> The government represents that it has already provided “a complete copy of the ACER laptop’s hard drive and a forensic report of its examination.” (Resp. at 5). To the extent that there are other factual reports generated by CERT as part of its forensic analysis, these reports must be produced as well. Moreover, as the government has agreed, the government shall make an “early identification of files, records and software code which it has determined to date may be material and offered as evidence at trial.” (Resp. at 5).

**2. Paragraph 12:** By this request, the defendant is seeking information concerning any attempt to see any information contained on the computer prior to the

---

<sup>1</sup> The government has not challenged the defendant’s assertion that the CERT computer analysis is material to the preparation of Swartz’s defense.

issuance of the search warrant in February 2011, on the grounds that “[m]oving a mouse or touching a key on a computer which reveals information that was not in plain view constitutes a search which may not be lawfully conducted under the Fourth Amendment in the absence of a valid warrant.” (Mot. at 3 (citing, inter alia, United States v. Musgrove, No. 11-CR-24, 2011 WL 4356515, at \*15 (E.D. Wis. Sept. 16, 2011))). However, as the government argues, the defendant “lost all reasonable expectation of privacy in the computer,” which was first located in a wiring closet in the basement of an MIT building hidden under a box and hard-wired into a computer switch, and later recovered at another location at MIT. (Resp. at 6). See United States v. Sanchez, 635 F.2d 47, 64 (2d Cir. 1980) (“a mere trespasser has no Fourth Amendment protection in premises he occupies wrongfully”). The government has apparently complied with its obligation to produce search materials as defined in Local Rule 116.1(C)(1)(b). Therefore, the motion to compel this additional material is denied.

**3. Paragraph 15:** In this request the defendant is seeking the “origin of any and all statements of Aaron Swartz” and “the legal procedure used to obtain each such statement[.]” (Mot. at 3). The purpose of the request is to enable Swartz “to move to suppress such statements if grounds exist to do so, which he cannot determine without the requested information.” (Mot. at 4). The government has confirmed that “[n]o emails, texts messages, chat logs, or documents were obtained from Internet service providers using orders under 18 U.S.C. 2703(d)” and that “there was no court-authorized electronic surveillance in this case.” (Resp. at 7). It has also confirmed that “[a]ll of the emails, text messages, chat sessions, and documents containing state-

ments provided by the defendant relevant to this case were obtained either from individuals with whom the defendant communicated or from publicly available websites stored on the Internet.” Id. The defendant does not explain why this information is not sufficient for him to decide if a motion to suppress is a viable alternative. The motion to compel the additional information is denied.

**4. Paragraphs 1, 4, 20:** In these paragraphs, Swartz is seeking all grand jury subpoenas and the documents produced in response to such subpoenas. According to the defendant, he is requesting this information “because some grand jury subpoenas used in this case contained directives to the recipients which Swartz contends were in conflict with Rule 6(e)(2)(A) . . . and others sought certification of the produced documents so that they could be offered into evidence under Fed. R. Evid. 803(6), 901. (Mot. at 4-5). Swartz requires the requested material “to determine whether there is a further basis for moving to exclude evidence under the Fourth Amendment (even though the SCA has no independent suppression remedy.” (Mot. at 5). He contends that the grand jury subpoenas may be “too sweeping” and that since the information was subpoenaed by an “experienced and respected senior prosecutor” the information must be material. (Id.). The government opposes these requests on the grounds that the defendant does not have standing to suppress the subpoenas, none of the subpoenas contained a “directive” to recipients of secrecy,<sup>2</sup> a conclusory

---

<sup>2</sup> The government has represented that the language used in letters accompanying some subpoenas was “We request that you not disclose the existence of the subpoena, or the fact of your compliance with it, to anyone. While you are not required to comply with this request, any such disclosure could impede the investigation and interfere with the enforcement of federal criminal law.” This language is consistent with instructions approved by the First

assertion that some subpoenas are too broad is not sufficient to justify the production of all subpoenas, and there is no support for the production of everything that a grand jury may have seen. (Resp. at 8-10). This court agrees. “A grand jury’s investigation is not fully carried out until every available clue has been run down and all witnesses examined in every proper way to find if a crime has been committed. . . .” United States v. Dionisio, 410 U.S. 1, 13, 93 S. Ct. 763, 771 (1973) (quotation omitted). At this juncture, the defendant has not stated a basis for such a sweeping production which exceeds the scope and timing requirements of the applicable rules.

**ORDER**

For all the reasons detailed herein, “Defendant Aaron Swartz’s Motion for Discovery” (Docket No. 40) is ALLOWED IN PART and DENIED IN PART. The government shall produce the materials required by this Order within 14 days of the date of this Order.

/ s / Judith Gail Dein  
\_\_\_\_\_  
JUDITH GAIL DEIN  
United States Magistrate Judge

---

Circuit. In re Grand Jury Proceedings(Diamonte), 814 F.2d 61,70 (1st Cir. 1987) (“The government is free to express its beliefs about the impact of any disclosure, provided it makes clear that the law does not require nondisclosure.”).

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4497384@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Order on Motion for Protective Order  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 8/1/2012 at 4:42 PM EDT and filed on 8/1/2012

**Case Name:** USA v. Swartz  
**Case Number:** 1:11-cr-10260-NMG  
**Filer:**  
**Document Number:** 47(No document attached)

**Docket Text:**

**Magistrate Judge Judith G. Dein: ELECTRONIC ORDER entered finding as moot [18] Motion for Protective Order as to Aaron Swartz (1); finding as moot [19] Motion to Compel as to Aaron Swartz (1); finding as moot [24] Motion as to Aaron Swartz (1); finding as moot [11] Motion to Unseal Document as to Aaron Swartz (1); finding as moot [13] Motion to Exclude as to Aaron Swartz (1) (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4497388@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Add and Terminate Judges  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 8/1/2012 at 4:43 PM EDT and filed on 8/1/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** No document attached

**Docket Text:**

**Judge update in case as to Aaron Swartz. Magistrate Judge Judith G. Dein no longer assigned to case. (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4497732@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Order on Report and Order on  
Final Status Conference by Magistrate Judge  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 8/2/2012 at 9:07 AM EDT and filed on 8/2/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** 48(No document attached)

**Docket Text:**

**Judge Nathaniel M. Gorton: ELECTRONIC ORDER entered acknowledging [44] Report and Order on Final Status Conference by Magistrate Judge as to Aaron Swartz (1) Interim Pretrial Conference set for 8/15/2012 02:30 PM in Courtroom 4 before Judge Nathaniel M. Gorton. (Patch, Christine)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**



MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4515902@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Initial pretrial Conference  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 8/15/2012 at 3:18 PM EDT and filed on 8/15/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** 49(No document attached)

**Docket Text:**

**ELECTRONIC Clerk's Notes for proceedings held before Judge Nathaniel M. Gorton: Interin Pretrial Conference as to Aaron Swartz held on 8/15/2012. Counsel anticipate trial lasting 2 weeks. Jury Trial set for 2/4/2013 09:00 AM in Courtroom 4 before Judge Nathaniel M. Gorton. Government's initial expert disclosures by 11/19/12, Defendant's by 12/10/12, and additional experts by 12/31/12. Motions in limine due by 1/14/2013; oppositions to Motions in Limine, Exhibit/Witness Lists, and proposed voir dire due by 1/21/2013; objections to exhibit/witness lists, proposed jury instructions, and proposed verdict form due by 1/21/2013. Government to file assented-to Motion to Exclude all time between 8/15/12 and 2/4/13. (Attorneys present: Weinberg, Heymann. )Court Reporter Name and Contact or digital recording information: Cheryl Dahlstrom (617-951-4555). (Patch, Christine)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4515906@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Terminate Deadlines and Hearings  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 8/15/2012 at 3:19 PM EDT and filed on 8/15/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** No document attached

**Docket Text:**

**Terminate Deadlines and Hearings as to Aaron Swartz: Interim Pretrial Conference held on 8/15/12. (Patch, Christine)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 11-10260-NMG
	)	
AARON SWARTZ,	)	
	)	
Defendant	)	

ASSENTED-TO MOTION FOR ORDER OF EXCLUDABLE DELAY  
PURSUANT TO THE SPEEDY TRIAL ACT

The United States of America moves for an order designating the period from August 15, 2012, through and including February 4, 2013, as excludable delay pursuant to the Speedy Trial Act, 18 U.S.C. §3161(h)(7)(A), on the grounds that the ends of justice served by granting the requested continuance of time outweigh the best interests of the public and the defendant in a speedy trial. Defendant Aaron Swartz, through counsel, fully assents to the allowing of this Motion. The parties anticipate the litigation of substantive motions in the case. The defendant requires additional time to prepare an effective defense, including time for expert analysis of the electronic evidence in this case, to prepare and litigate the substantive and other motions and to consider how best to present his defense at trial. Not granting this continuance would deny defense counsel a reasonable time necessary for effective preparation. See 18 U.S.C. §3161(h)(7)(B)(ii).

Respectfully submitted,

Carmen M. Ortiz  
United States Attorney

/s/ Martin G. Weinberg  
MARTIN G. WEINBERG  
Counsel for Defendant  
Aaron Swartz

By: /s/ Stephen P. Heymann  
STEPHEN P. HEYMANN  
SCOTT L. GARLAND  
Assistant U.S. Attorneys

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to  
Martin G. Weinberg, Esq..

/s/ Stephen P. Heymann  
STEPHEN P. HEYMANN  
Assistant United States Attorney

Date: August 17, 2012

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4527620@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Order on Motion for Speedy Trial  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 8/24/2012 at 11:02 AM EDT and filed on 8/24/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** 51(No document attached)

**Docket Text:**

**Judge Nathaniel M. Gorton: ELECTRONIC ORDER entered granting [50] Motion for Speedy Trial as to Aaron Swartz (1) (Patch, Christine)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA

MAG. JUDGE NO. \_\_\_\_\_

V.

CRIMINAL NO. 11-10260-NMGAARON SWARTZ

ORDER OF EXCLUDABLE DELAY

In accordance with the Speedy Trial Act of 1974, as amended, this Court hereby orders excludable delay for the time periods and for the reasons checked below.

8/24/2012  
Date

/s/ Nathaniel M. Gorton

U.S. District Judge [✓]

U.S. Magistrate Judge [ ]

REFER TO DOCUMENT(S) # 50

<input type="checkbox"/>	XA	_____	Proceedings including examinations to determine mental competency or physical capacity	18 U.S.C. § 3161(h)(1)(A)
<input type="checkbox"/>	XC	_____	Trial on other charges against defendant	18 U.S.C. § 3161(h)(1)(B)
<input type="checkbox"/>	XD	_____	Interlocutory Appeal	18 U.S.C. § 3161(h)(1)(C)
<input type="checkbox"/>	XE	_____	Pretrial motions from filing date to hearing or disposition	18 U.S.C. § 3161(h)(1)(D)
<input type="checkbox"/>	XF	_____	Transfer (Rule 20) or Removal (Rule 40) proceedings	18 U.S.C. § 3161(h)(1)(E)
<input type="checkbox"/>	XG	_____	Proceedings under advisement	18 U.S.C. § 3161(h)(1)(H)
<input type="checkbox"/>	XH	_____	Miscellaneous proceedings concerning defendant	18 U.S.C. § 3161(h)(1)
<input type="checkbox"/>	XI	_____	Prosecution deferred	18 U.S.C. § 3161(h)(2)
<input type="checkbox"/>	XJ	_____	Transportation from other district	18 U.S.C. § 3161(h)(1)(F)
<input type="checkbox"/>	XK	_____	Consideration of proposed plea agreement	18 U.S.C. § 3161(h)(1)(G)
<input type="checkbox"/>	XM	_____	Absence or unavailability of defendant or essential government witness	18 U.S.C. § 3161(h)(3)
<input type="checkbox"/>	XN	_____	Period of mental or physical incompetency or physical inability to stand trial	18 U.S.C. § 3161(h)(4)
<input type="checkbox"/>	XP	_____	Superseding indictment and/or new charges	18 U.S.C. § 3161(h)(5)
<input type="checkbox"/>	XR	_____	Defendant joined with co-defendant for whom time has not run	18 U.S.C. § 3161(h)(6)
<input type="checkbox"/>	XU	_____	Time from first arraignment to withdrawal of guilty plea	18 U.S.C. § 3161(i)
<input type="checkbox"/>	XW	_____	Grand Jury indictment time extended	18 U.S.C. § 3161(b)
<input checked="" type="checkbox"/>	XT	<u>8/15/12 - 2/4/13</u>	Continuance granted in the interest of justice	18 U.S.C. § 3161(h)(7)(A)

**UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS**

**UNITED STATES OF AMERICA**

**v.**

**AARON SWARTZ,**

**Defendant**

**Crim. No. 11-CR-10260-NMG**

**VIOLATIONS:**

**18 U.S.C. § 1343 (Wire Fraud)**

**18 U.S.C. § 1030(a)(4),(b) (Computer Fraud)**

**18 U.S.C. § 1030(a)(2), (b), (c)(2)(B)(iii)  
(Unlawfully Obtaining Information from a  
Protected Computer)**

**18 U.S.C. § 1030(a)(5)(B), (c)(4)(A)(i)(I),(VI)  
(Recklessly Damaging a Protected Computer)**

**18 U.S.C. § 2 (Aiding and Abetting)**

**18 U.S.C. § 981(a)(1)(C), 28 U.S.C. § 2461(c),  
18 U.S.C. § 982(a)(2)(B), and 18 U.S.C. §  
1030(i) (Criminal Forfeiture)**

**SUPERSEDING INDICTMENT**

The Grand Jury charges that at all relevant times:

***PARTIES***

***JSTOR***

1. JSTOR, founded in 1995, was and continued to be a United States-based, not-for-profit organization that provides an online system for archiving and providing access to academic journals and journal articles. It provides searchable digitized copies of articles from over 1,000 academic journals, dating back for lengthy periods of time.

2. JSTOR's service is important to research institutions and universities because it can be extraordinarily expensive, in terms of both cost and space, for a research or university library to maintain a comprehensive collection of academic journals. By digitizing extensive, historical collections of journals, JSTOR enables libraries to outsource the journals' storage, ensures their preservation, and enables authorized users to conduct full-text, cross-disciplinary

searches of them. JSTOR has invested millions of dollars in obtaining and digitizing the journal articles that it makes available as part of its service.

3. JSTOR generally charges libraries, universities, and publishers a subscription fee for access to JSTOR's digitized journals. For a large research university, this annual subscription fee for JSTOR's various collections of content can cost more than \$50,000. Portions of the subscription fees are shared with the journal publishers who hold the original copyrights. In addition, JSTOR makes some articles available for individual purchase.

4. JSTOR authorizes users to download a limited number of journal articles at a time. Before being given access to JSTOR's digital archive, each user must agree and acknowledge that they cannot download or export content from JSTOR'S computer servers with automated computer programs such as web robots, spiders, and scrapers. JSTOR also uses computerized measures to prevent users from downloading an unauthorized number of articles using automated techniques.

***MIT***

5. The Massachusetts Institute of Technology ("MIT") was and continued to be a leading research and teaching university located in Cambridge, Massachusetts.

6. JSTOR provided MIT with its services and content for a fee.

7. MIT made JSTOR's services and content available to its students, faculty, and employees. MIT also allowed guests of the Institute to have the same access to JSTOR, but required guests to register on the MIT network. MIT authorized guests to use its network for no more than fourteen days per year, and required all users to use the network to support MIT's research, education, and administrative activities, or at least to not interfere with these activities; to maintain the system's security and conform to applicable laws, including copyright laws; and to conform with rules imposed by any networks to which users connected through MIT's system. These rules explicitly notified users that violations could lead to state or federal prosecution. Guest users of the MIT network agreed to be bound by the same rules that applied to students,



faculty, and employees.

8. JSTOR's computers were located outside the Commonwealth of Massachusetts, and thus any communications between JSTOR's computers and MIT's computers crossed state boundaries. JSTOR's and MIT's computers were also used in and affected interstate and foreign commerce.

***Aaron Swartz***

9. Aaron Swartz lived in the District of Massachusetts and was a fellow at Harvard University's Safra Center for Ethics. Swartz was not affiliated with MIT as a student, faculty member, or employee or in any other manner. Although Harvard provided Swartz access to JSTOR's services and archive as needed for his research, Swartz used MIT's computer networks to steal millions of articles from JSTOR.

***OVERVIEW OF THE OFFENSES***

10. Between September 24, 2010, and January 6, 2011, Swartz contrived to:
  - a. break into a restricted-access computer wiring closet at MIT;
  - b. access MIT's network without authorization from a switch within that closet;
  - c. access JSTOR's archive of digitized journal articles through MIT's computer network;
  - d. use this access to download a substantial portion of JSTOR's total archive onto his computers and computer hard drives;
  - e. avoid MIT's and JSTOR's efforts to prevent this massive copying, efforts that were directed at users generally and at Swartz's illicit conduct specifically; and
  - f. elude detection and identification.

***MEANS OF COMMITTING THE OFFENSES***

11. Swartz alone, or in knowing concert with others unknown to the Grand Jury, (hereafter simply “Swartz” in this section) committed these offenses through the means described below.

***September 24 through 27, 2010***

12. On September 24, 2010, Swartz purchased an Acer laptop computer from a local computer store.

13. Later that day, Swartz connected the Acer laptop to MIT’s computer network from a location in Building 16 at MIT and registered with MIT’s computer network as a guest.

14. When Swartz registered on the network, he took measures to hide his identity as the computer’s owner and user:

- a. Swartz registered the computer under the fictitious guest name “Gary Host.”
- b. Swartz specified the computer’s client name as “ghost laptop.” (A computer’s client name helps to identify it on a network and can be chosen by its user.) In this case, the “ghost” client name abridged the pseudonym “Gary Host” by combining the first initial “g” with the last name “host.”
- c. Swartz identified the fictitious “Gary Host’s” e-mail address as “ghost@mailinator.com”, a temporary e-mail address. Mailinator advertised itself as a free e-mail service that allows a user to create a new temporary-mail address as needed. Mailinator advertised that it would accept mail for any e-mail address directed to the mailinator.com domain without need for a prior registration or account. Mailinator also advertised that all mail sent to mailinator.com would automatically be deleted after several hours, whether read or not, and that the company kept no logs of e-mail access.

15. On September 25, 2010, Swartz used the Acer laptop to systematically access and

rapidly download an extraordinary volume of articles from JSTOR by submitting download requests faster than a human could type, and in a manner designed to sidestep or confuse JSTOR's computerized efforts to restrict the volume of individual users' downloads.

16. The effect of these rapid and massive downloads and download requests was to impair computers used by JSTOR to provide articles to client research institutions.

17. As JSTOR, and then MIT, became aware of these events, each took steps to block communications to and from Swartz's computer. Swartz, in turn, altered the apparent source of his automated demands to sidestep or circumvent JSTOR's and MIT's blocks against his computer, as described below:

- a. On the evening of September 25, 2010, JSTOR terminated Swartz's computer's network access by refusing communications from the computer's assigned IP address.
  - i. An IP (short for "Internet Protocol") address is a unique numeric address assigned to each computer connected to the Internet so that the computer's incoming and outgoing Internet traffic is directed to the proper destination. Most Internet service providers control a range of IP addresses. MIT controls all IP addresses that begin with the number 18.
  - ii. Swartz's computer had been assigned an IP address of 18.55.6.215.
  - iii. On September 25, 2010, JSTOR blocked communications from that IP address, thus preventing Swartz from requesting and receiving any more JSTOR articles.
- b. On September 26, 2010, Swartz established a new IP address for his computer on the MIT network – 18.55.6.216 – which sidestepped the IP address block and allowed the laptop to resume downloading an extraordinary volume of articles from JSTOR. Accesses from this address continued until the middle of the day, when JSTOR spotted the access and blocked communications from this

new IP address as well.

c. Because the downloads on September 25 and 26 originated from shifting MIT IP addresses beginning with 18.55.6, and because JSTOR's computers used to provide articles to research institutions had been impaired and significant portions of its archive was at risk of misappropriation, on September 26, 2010, JSTOR began blocking a broader range of IP addresses. The block prevented a researcher assigned any one of over 250 other IP addresses available at MIT from being able to access JSTOR's archive until September 29, 2010.

d. After JSTOR notified MIT what was happening, MIT sought to block Swartz in particular. It did so by prohibiting Swartz's laptop from being assigned any IP address on MIT's network. MIT did so by blocking communications with any computer bearing the laptop's MAC address.

i. A MAC address is a unique identifier assigned to each computer's network interface, in this case, Swartz's Acer laptop's network interface card.

ii. When a user plugs his computer into MIT's wired network on campus, the network reads the computer's MAC address to determine whether the computer is authorized to use the network. As part of the registration process, "Gary Host's" computer, i.e., Swartz's Acer laptop, had identified its network interface's MAC address as 00:23:5a:73:5f:fb.

iii. Consequently, on September 27, 2010, MIT terminated the laptop's guest registration and barred any network interface with that MAC address from obtaining a new IP address.

***October 2 through 9, 2010***

18. On October 2, 2010, just over a week after JSTOR and MIT had blocked Swartz's Acer laptop from communicating with JSTOR's and MIT's networks, Swartz sought and

obtained another guest connection on MIT's network for his Acer laptop.

19. Once again, Swartz registered the Acer laptop on the network using identifiers chosen to avoid identifying Swartz as the computer's owner and user:

- a. Swartz once again registered the computer under the fictitious name "Gary Host" and the client name "ghost laptop."
- b. To evade the MAC address block, Swartz "spoofed" the Acer laptop's computer's MAC address. A MAC address is usually assigned to a network interface card by the card's manufacturer, and therefore generally remains constant. But a user with the right knowledge can change the MAC address, an action referred to as "MAC address spoofing." Swartz spoofed the Acer laptop's MAC address by changing it from 00:23:5a:73:5f:fb to 00:23:5a:73:5f:fc (that is, the final 'b' became a 'c').
- c. By re-registering the laptop, the laptop received a new IP address, which disassociated Swartz's Acer laptop from the IP addresses that JSTOR had blocked when Swartz had used them in September.

20. On October 8, 2010, Swartz connected a second computer to MIT's network and registered as a guest, using similar naming conventions: Swartz registered the computer under the name "Grace Host," the computer client name "ghost macbook," and the temporary e-mail address "ghost42@mailinator.com."

21. On October 9, 2010, Swartz used both the "ghost laptop" and the "ghost macbook" to, again, systematically and rapidly access and download articles from JSTOR. The pace of Swartz's automated downloads was so fast and voluminous that it significantly impaired the operation of some computers at JSTOR.

22. In response, beginning on or about October 9, 2010, JSTOR blocked MIT's entire computer network from accessing JSTOR. The block lasted several days, again depriving legitimate users at MIT from accessing JSTOR's services.



***November and December, 2010***

23. During November and December, 2010, Swartz again used the “ghost laptop” (i.e., the Acer laptop) at MIT to download over two million documents from JSTOR, more than one hundred times the number of downloads during the same period by all legitimate MIT JSTOR users combined.

24. During this period, when Swartz connected to MIT’s computer network, he circumvented MIT’s guest registration process altogether. Rather than let MIT assign his computer an IP address automatically, Swartz instead simply hard-wired into the network and assigned himself two IP addresses. He did so by entering a restricted network interface closet in the basement of MIT’s Building 16, plugging the computer directly into the network, and operating the computer to assign itself two IP addresses. To further cloak his activities, Swartz also hid the Acer laptop and a succession of external storage drives under a box in the closet, so that they would not arouse the suspicions of anyone who might enter the closet.

***January 4 through 6, 2011***

25. On January 4, 2011, Swartz entered the restricted basement network wiring closet and replaced an external hard drive attached to the laptop.

26. On January 6, 2011, Swartz returned to the wiring closet to remove his computer equipment. This time he attempted to evade identification at the entrance to the restricted area. Apparently aware of or suspicious of a video camera, as Swartz entered the wiring closet, he held his bicycle helmet like a mask to shield his face, looking through ventilation holes in the helmet. Swartz then removed his computer equipment from the closet, put it in his backpack, and left, again masking his face with the bicycle helmet before peering through a crack in the double doors and cautiously stepping out.

27. Later that day, Swartz connected his Acer laptop to MIT’s network in a different building — the student center — again registering on the network using identifiers chosen to avoid identifying Swartz as the computer’s owner and user:

- a. Swartz registered the computer under the fictitious name "Grace Host" and the client name "ghost laptop."
- b. By re-registering the laptop, the laptop again received a new IP address, which disassociated Swartz's Acer laptop from the IP addresses Swartz had used up to that point.
- c. To again evade the MAC address block, Swartz had spoofed the Acer laptop's MAC address a second time, changing it from the blocked 00:23:5a:73:5f:fb (or from the later-spoofed 00:23:5a:73:5f:fc) to 00:4c:e5:a0:c7:56.

28. Swartz's Acer laptop contained a software program named "keepgrabbing.py," which was designed to download .pdf files (the format used by JSTOR) from JSTOR and sidestep or confuse JSTOR's computerized efforts to prevent repeated and voluminous downloads.

29. When MIT Police spotted Swartz on the afternoon of January 6, 2011 and attempted to question him, Swartz fled with a USB drive that contained the program "keepgrabbing2.py," which was similar to "keepgrabbing.py."

30. In all, Swartz stole a major portion of the total archive in which JSTOR had invested.

31. Swartz intended to distribute these articles through one or more file-sharing sites.

**COUNTS 1 and 2  
Wire Fraud  
18 U.S.C. §§ 1343 & 2**

32. The Grand Jury realleges and incorporates by reference the allegations in paragraphs 1-31 of this Indictment.

33. Aaron Swartz devised a scheme to defraud JSTOR of a substantial number of journal articles which they had invested in collecting, obtaining the rights to distribute, and digitizing.

34. He sought to defraud MIT and JSTOR of rights and property by:

- a. Deceptively making it appear to JSTOR that he was affiliated with MIT by downloading JSTOR's articles through MIT's computer network and from MIT IP addresses, even though he was not affiliated at the time with MIT, and even though for legitimate research he could have accessed JSTOR through Harvard University, where he worked;
- b. Repeatedly taking steps to change his and his computer's apparent identities and to conceal his and his computer's true identities;
- c. Using a rapid, automated collection software tool designed to make it appear as if he were multiple people making single requests rather than a single person making multiple requests, in order to bypass safeguards designed to limit the number of articles any one person could download;
- d. Attempting to conceal from MIT the physical location of the Acer laptop's connection to MIT's network, by placing it in a utility closet, covering it with cardboard, and, at one point, moving it from one MIT building to another; and
- e. Using wire communications between a MIT computer in Massachusetts and JSTOR's computer out-of-state to effectuate his scheme.

35. The Grand Jury charges that repeatedly from on or about September 24, 2010 through January 6, 2011, or thereabout, in the District of Massachusetts and elsewhere, the



defendant,

**AARON SWARTZ,**

having devised and intended to devise a scheme and artifice to defraud and for obtaining property — journal articles digitized and distributed by JSTOR, and copies of them — by means of material false and fraudulent pretenses and representations, transmitted and caused to be transmitted by means of wire communication in interstate commerce writings, signs, and signals — that is, communications to and from JSTOR's computer servers —for the purpose of executing the scheme, and aiding and abetting it, including on or about the dates specified below:

COUNT	DATES
1	October 9, 2010
2	January 4-6, 2011

All in violation of Title 18, United States Code, Sections 1343 and 2.

**COUNTS 3-7**  
**Computer Fraud**  
**18 U.S.C. §§ 1030(a)(4), (b) & 2**

36. The Grand Jury realleges and incorporates by reference the allegations in paragraphs 1-31 and 33-34 of this Indictment and charges that:

37. Repeatedly between on or about September 26, 2010 and January 6, 2011, including on or about the dates specified below, in the District of Massachusetts and elsewhere, the defendant,

**AARON SWARTZ,**

knowingly and with intent to defraud, accessed protected computers belonging to MIT and JSTOR without authorization, and by means of such conduct furthered the intended fraud and obtained things of value — namely, digitized journal articles from JSTOR's archive — and aided and abetted the same and attempted to do the same:

<b>COUNT</b>	<b>DATES</b>	<b>PROTECTED COMPUTERS</b>
3	September 26, 2010	JSTOR
4	October 2-9, 2010	MIT
5	November 29, 2010 - December 26, 2010	JSTOR
6	December 27, 2010 - January 4, 2011	JSTOR
7	January 4-6, 2011	MIT

All in violation of Title 18, United States Code, Sections 1030(a)(4) and 2.

**COUNT 8-12**  
**Unlawfully Obtaining Information from a Protected Computer**  
**18 U.S.C. §§ 1030(a)(2), (b), (c)(2)(B)(iii) & 2**

38. The Grand Jury realleges and incorporates by reference the allegations in paragraphs 1-31 and 33-34 of this Indictment and charges that:

39. Repeatedly between September 26, 2010 and January 6, 2011, including on or about the dates specified below, in the District of Massachusetts and elsewhere, the defendant,

**AARON SWARTZ,**

intentionally accessed computers belonging to MIT and JSTOR without authorization, and thereby obtained from protected computers information whose value exceeded \$5,000 — namely, digitized journal articles from JSTOR's archive — and aided and abetted the same and attempted to do the same.

<b>COUNT</b>	<b>DATES</b>	<b>PROTECTED COMPUTERS</b>
8	September 26, 2010	JSTOR
9	October 2-9, 2010	MIT
10	November 29, 2010 - December 26, 2010	JSTOR
11	December 27, 2010 - January 4, 2011	JSTOR
12	January 4-6, 2011	MIT

All in violation of 18 U.S.C. §§ 1030(a)(2), (c)(2)(B)(iii) and 2.

**COUNT 13**  
**Recklessly Damaging a Protected Computer**  
**18 U.S.C. §§ 1030(a)(5)(B), (c)(4)(A)(i)(I),(VI) & 2**

40. The Grand Jury realleges and incorporates by reference the allegations in paragraphs 1-31 and 33-34 of this Indictment.

41. Aaron Swartz's repeated accessing of JSTOR's and MIT's computer systems without authorization constituted a related course of conduct lasting from on or about September 26, 2010 through January 6, 2011. His unauthorized access of the systems on or about days such as September 26 and October 9, 2010 resulted in reckless damage to both. The pace and volume of his automated requests impaired computers JSTOR used to provide service to researchers and research institutions and caused JSTOR to cut off legitimate MIT researchers for days at a time.

42. Both MIT and JSTOR were required to expend significant resources to respond to Swartz's unlawful access to their systems and high speed automated downloads of substantial portions of JSTOR's digital archives.

43. The Grand Jury charges that on or about October 9, 2010 in the District of Massachusetts and elsewhere, the defendant,

**AARON SWARTZ,**

intentionally accessed a protected computer without authorization, and as a result of such conduct recklessly caused damage to MIT and JSTOR, that is impairment to the availability of information, data, and a system, which, during a one year period:

- (A) caused loss, that is, reasonable costs of responding to the offense, conducting a damage assessment, and restoring the information, data, and system to its condition prior to the offense, aggregating at least \$5,000 in value from a related course of conduct affecting at least one other protected computer, and
- (B) damage affecting at least 10 protected computers.

All in violation of Title 18, United States Code, Section 1030(a)(5)(B), (c)(4)(A)(i)(I),(VI) & 2.

**FORFEITURE ALLEGATIONS**  
**(18 U.S.C. § 981(a)(1)(C), 28 U.S.C. § 2461(c), 18 U.S.C. § 982(a)(2)(B), and 18 U.S.C. § 1030(i))**

44. Upon conviction of one or more of the offenses alleged in Counts One and Two of the Indictment, the defendant,

**AARON SWARTZ,**

shall forfeit to the United States, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), any property, real or personal, that constitutes, or is derived from, proceeds traceable to the commission of the offense.

45. Upon conviction of one or more of the offenses alleged in Counts Three through Thirteen of the Indictment, the defendant,

**AARON SWARTZ,**

shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(2)(B) and 18 U.S.C. § 1030(i) any property constituting, or derived from, proceeds obtained directly or indirectly as a result of the commission of the offenses, and pursuant to 18 U.S.C. § 1030(i) any personal property that was used or intended to be used to commit or facilitate the commission of such violations.

46. If any of the property described in paragraphs 44 and 45 hereof as being forfeitable pursuant to 18 U.S.C. § 981(a)(1)(C), 28 U.S.C. § 2461(c), 18 U.S.C. § 982(a)(2)(B), and 18 U.S.C. § 1030(i) as a result of any act or omission of the defendant --

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred to, sold to, or deposited with a third party;
- c. has been placed beyond the jurisdiction of this Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

it is the intention of the United States, pursuant to 21 U.S.C. § 853(p), as incorporated by 28 U.S.C. § 2461(c), 18 U.S.C. § 982(b)(1), and 18 U.S.C. § 1030(i)(2), to seek forfeiture of all

other property of the defendant up to the value of the property described in paragraphs 44 and 45 above.

All pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 982(a)(2)(B), and 1030(i), and Title 28, United States Code, Section 2461(c).

A TRUE BILL

Brenda L. Fannon  
Foreperson of the Grand Jury

Scott L. Dink  
Assistant United States Attorney

Date: 9-12-12

DISTRICT OF MASSACHUSETTS

September 12, 2012

Returned into the District Court by the Grand Jurors and filed.

Steve Yook  
Deputy Clerk

12:43 9/12/12

**Criminal Case Cover Sheet**

**U.S. District Court - District of Massachusetts**

Place of Offense: \_\_\_\_\_ Category No. II Investigating Agency \_\_\_\_\_ Secret Service \_\_\_\_\_

City Cambridge Related Case Information:

County Middlesex Superseding Ind./ Inf. \_\_\_\_\_ Superseding Ind. \_\_\_\_\_ Case No. 11-CR-10260-NMG

Same Defendant Yes New Defendant \_\_\_\_\_

Magistrate Judge Case Number \_\_\_\_\_

Search Warrant Case Number \_\_\_\_\_ See Additional Information Below \_\_\_\_\_

R 20/R 40 from District of \_\_\_\_\_

**Defendant Information:**

Defendant Name Aaron Swartz Juvenile: ☐ Yes ☒ No

Is this person an attorney and/or a member of any state/federal bar: ☐ Yes ☒ No

Alias Name \_\_\_\_\_

Address (City & State) Cambridge, MA

Birth date (Yr only): 86 SSN (last4#): 1374 Sex M Race: W Nationality: USA

Defense Counsel if known: Martin Weinberg, Esq. Address 20 Park Plaza

Bar Number \_\_\_\_\_ Suite 1000

U.S. Attorney Information: \_\_\_\_\_ Boston, MA 02116

AUSA Stephen P. Heymann & Scott L. Garland Bar Number if applicable 558486 & 650358

Interpreter: ☐ Yes ☒ No List language and/or dialect: \_\_\_\_\_

Victims: ☒ Yes ☐ No If yes, are there multiple crime victims under 18 USC§3771(d)(2) ☒ Yes ☐ No

Matter to be SEALED: ☐ Yes ☒ No

☐ Warrant Requested ☒ Regular Process ☐ In Custody

**Location Status:**

Arrest Date \_\_\_\_\_

☐ Already in Federal Custody as of \_\_\_\_\_ in \_\_\_\_\_

☐ Already in State Custody at \_\_\_\_\_ ☐ Serving Sentence ☐ Awaiting Trial

☒ On Pretrial Release: Ordered by: Magistrate Judge Dein on 7/19/11

Charging Document: ☐ Complaint ☐ Information ☒ Indictment

Total # of Counts: ☐ Petty \_\_\_\_\_ ☐ Misdemeanor \_\_\_\_\_ ☒ Felony 13

Continue on Page 2 for Entry of U.S.C. Citations

☒ I hereby certify that the case numbers of any prior proceedings before a Magistrate Judge are accurately set forth above.

Date: September 12, 2012 Signature of AUSA: Scott L. Garland



District Court Case Number (To be filled in by deputy clerk): \_\_\_\_\_

Name of Defendant Aaron Swartz

## U.S.C. Citations

	<u>Index Key/Code</u>	<u>Description of Offense Charged</u>	<u>Count Numbers</u>
Set 1	<u>18 USC 1343</u>	<u>Wire Fraud</u>	<u>1-2</u>
Set 2	<u>18 USC 1030(a)(4)</u>	<u>Computer Fraud</u>	<u>3-7</u>
Set 3	<u>18 USC 1030(a)(2)</u>	<u>Theft of Information From a Computer</u>	<u>8-12</u>
Set 4	<u>18 USC 1030(a)(5)(B)</u>	<u>Recklessly Damaging a Computer</u>	<u>13</u>
Set 5	<u>18 USC 981, 982, 1030 &amp; 28 USC 2461</u>	<u>Forfeiture</u>	
Set 6	<u>18 USC 2</u>	<u>Aiding and Abetting</u>	<u>1-13</u>
Set 7	_____	_____	_____
Set 8	_____	_____	_____
Set 9	_____	_____	_____
Set 10	_____	_____	_____
Set 11	_____	_____	_____
Set 12	_____	_____	_____
Set 13	_____	_____	_____
Set 14	_____	_____	_____
Set 15	_____	_____	_____

**ADDITIONAL INFORMATION:** Search Warrant Case Numbers: 11m-5013-JGD; 11m-5014-JGD  
11m-5015-JGD; 11m-5031-JGD; 11m-5061-JGD; 11m-5062-JGD; 11m-5063-JGD; and  
11m-5143-JGD

**Seizure Warrant Case Number:** 11m-5138-JGD



MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4553624@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Order Referring Case to  
Magistrate Judge  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 9/12/2012 at 1:50 PM EDT and filed on 9/12/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** 54(No document attached)

**Docket Text:**

**Judge Nathaniel M. Gorton: ELECTRONIC ORDER entered. Order Referring Case to  
Magistrate Judge Judith G. Dein Reason for referral: P as to Aaron Swartz (Smith3, Dianne)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES	)	
	)	
v.	)	No. 11-10260-NMG
	)	
AARON SWARTZ	)	
	)	

**ASSENTED-TO MOTION TO AMEND PRETRIAL BRIEFING SCHEDULE**

Now comes the defendant Aaron Swartz and respectfully moves that the deadlines for filing pretrial motions set forth in the Final Status Report, August 1, 2012 (Doc. 44), which were established before the return of the Superceding Indictment on September 12, 2012, be extended for both the defendant and the government, such that the defendant's motions will be due on October 5, 2012, and the government's responses will be due on November 13, 2012.

As reason therefor, defendant states that the additional week for the filing of motions he is requesting is necessary in light of the number and complexity of the motions to be filed.

Counsel has conferred with AUSA Stephen Heymann, who assents to the granting of this motion.

Respectfully submitted,  
By his attorney,

/s/ Martin G. Weinberg  
Martin G. Weinberg  
20 Park Plaza, Suite 1000  
Boston, MA 02116  
(617) 227-3700 (tel.)  
(617) 338-9538 (fax)  
owlmgw@att.net

**CERTIFICATE OF SERVICE**

I, Martin G. Weinberg, hereby certify that on this 14th day of September, 2012, a copy of the foregoing document has been served via the Court's ECF system on all registered participants, including Stephen P. Heymann, AUSA.

**/s/ Martin G. Weinberg**

Martin G. Weinberg

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4565739@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Notice of Hearing  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 9/20/2012 at 9:54 AM EDT and filed on 9/20/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** 56(No document attached)

**Docket Text:**

**ELECTRONIC NOTICE OF HEARING as to Aaron Swartz Arraignment set for 9/24/2012 11:00 AM in Courtroom 15 before Magistrate Judge Judith G. Dein. (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4574125@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Arraignment  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 9/25/2012 at 5:01 PM EDT and filed on 9/24/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** 57(No document attached)

**Docket Text:**

**ELECTRONIC Clerk's Notes for proceedings held before Magistrate Judge Judith G. Dein:Arraignment as to Aaron Swartz (1) Count 1s-2s,3s-7s,8s-12s,13s held on 9/24/2012, Plea entered by Aaron Swartz Not Guilty on counts all. (Attorneys present: Garland and Weinberg. )Court Reporter Name and Contact or digital recording information: Digital Recording – for transcripts or CDs contact Deborah Scalfani (deborah\_scalfani@mad.uscourts.gov). (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4574139@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Order on Motion for Extension of Time  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 9/25/2012 at 5:03 PM EDT and filed on 9/24/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** 58(No document attached)

**Docket Text:**

**Magistrate Judge Judith G. Dein: ELECTRONIC ORDER entered granting [55] Motion for Extension of Time as to Aaron Swartz (1) (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4574149@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Add and Terminate Judges  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 9/25/2012 at 5:06 PM EDT and filed on 9/25/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** No document attached

**Docket Text:**

**Judge update in case as to Aaron Swartz. Magistrate Judge Judith G. Dein no longer assigned to case. (Quinn, Thomas)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES	)	
	)	
v.	)	No. 11-10260-NMG
	)	
AARON SWARTZ	)	

**MOTION TO SUPPRESS ALL FRUITS OF INTERCEPTIONS AND DISCLOSURES OF  
ELECTRONIC COMMUNICATIONS AND OTHER INFORMATION BY MIT  
PERSONNEL IN VIOLATION OF THE FOURTH AMENDMENT AND THE STORED  
COMMUNICATIONS ACT AND INCORPORATED MEMORANDUM OF LAW  
(MOTION TO SUPPRESS NO. 1)**

Now comes the defendant Aaron Swartz and respectfully moves that this Honorable Court suppress as evidence at the trial of this case (1) the network flow data and DHCP logs collected by MIT personnel and disclosed to the government without a warrant or court order or subpoena, as well as all evidence derived therefrom, and (2) all evidence from the packet capture instituted by MIT personnel on the morning of January 4, 2011, and continuing, at the request of the government that MIT personnel continue to intercept electronic communications, through January 6, 2011, and subsequently turned over to the Secret Service, as well as all evidence derived therefrom.<sup>1</sup>

As reason therefor, defendant states:

---

<sup>1</sup> In a separate motion to suppress, Swartz contends that after law enforcement agents arrived on the scene on January 4, 2011, and recommended that MIT personnel continue the packet capture they had begun earlier that morning and began to direct the investigation, MIT personnel were acting as government agents, and their actions were therefore subject to the requirements of the Fourth Amendment. *See* Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law. This motion is directed in part at the interceptions conducted by MIT personnel before they began acting as government agents, as well as MIT's turning over to the government material in which Swartz had a reasonable expectation of privacy, in the complete absence of judicial process compelling MIT to produce such evidence to the government at a time when law enforcement agents were directing MIT employees regarding how to further their criminal investigation of the defendant.



1. He had a reasonable expectation of privacy in the electronic communications flowing to and from his ACER netbook.<sup>2</sup>

2. The interception of network flow data to the netbook and the packet capture constituted interceptions of electronic communications within the meaning of Title III.

3. The interceptions conducted by MIT and its disclosure of the information gathered to the Secret Service violated 18 U.S.C. §2511(1), as no exceptions to the requirements of Title III apply to MIT's conduct. The evidence, along with all derivative fruits thereof, must, therefore, be suppressed as violative of the Fourth Amendment.

4. The disclosure of DHCP logs by MIT personnel in the absence of a warrant issued upon a showing of probable cause or a court order pursuant to 18 U.S.C. §2703(d) violated the Fourth Amendment and/or the Stored Communications Act.

5. MIT's disclosure to the Secret Service of DHCP logs, network flow data, and packet capture information in the absence of a subpoena or search warrant violated 18 U.S.C. §§2702, 2703, as well as Swartz's rights under the Fourth Amendment such that suppression of the evidence, as well as all derivative fruits, is required.

**THE DEFENDANT REQUESTS A HEARING ON THE WITHIN MOTION.**

**LOCAL RULE 7.1(A)(2) STATEMENT**

The undersigned counsel has conferred with AUSA Stephen Heymann. The government opposes the suppression remedies sought and will respond to defendant's request for a hearing in its response to the motion.

---

<sup>2</sup> All averments herein regarding Swartz's ownership and possession of the ACER netbook and the attached hard drive, and the communications flowing to and from them, are made pursuant to the protections provided by *Simmons v. United States*, 390 U.S. 377, 392-94 (1968).

## MEMORANDUM OF LAW

### I. FACTUAL BACKGROUND.

On September 26, 2010, MIT received an email from Brian Larsen at JSTOR, an online archive of scholarly journal articles, informing it that there had been, that morning, an excessive downloading of journals. By the next day, the IP addresses from which the journals were being downloaded had been located (largely, if not exclusively, by JSTOR) and the user information for the guest registration of the computer being used had been identified; JSTOR then blocked access to these IP addresses. Timeline of events related to JSTOR downloading incident: 9/26/10 - 1/6/11, Exhibit 1 (“Timeline”) at 1. On October 9, 2010, JSTOR again notified MIT that its access was being blocked because of excessive downloading. Timeline at 2. JSTOR quickly identified the IP address being used for the downloads, and MIT personnel thereafter discovered that access was being accomplished in Building 16 by a computer registered through its visitor guest registration process by the same guest whose computer was linked to the September incident.<sup>3</sup> Timeline at 2-3.

MIT and JSTOR conferred regarding methods to prevent excessive downloading. Timeline at 3-4. On December 26, 2010, there was another episode of excessive downloading, which MIT personnel did not learn of until on or about January 3, 2011. On the morning of January 4, 2011, at approximately 8:00 am, MIT personnel located the netbook being used for the downloads and decided to leave it in place and institute a packet capture of the network traffic to and from the netbook.<sup>4</sup> Timeline at 6. This was accomplished using the laptop of Dave Newman, MIT Senior

---

<sup>3</sup> MIT personnel first received notice of the October 9, 2010, incident when they returned following the Columbus Day holiday on October 12, 2010. Timeline at 2.

<sup>4</sup> A packet capture captures the entire communication, including subject matter and content, and to the extent it was diverting and copying communications in transit to and from the netbook, this constituted a classic interception of electronic communications in violation of *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005)(*en banc*). See page 9, *infra*.

Network Engineer, which was connected to the netbook and intercepted the communications coming to and from it. *Id.* Later that day, beginning at 11:00 am, the Secret Service assumed control of the investigation.<sup>5</sup> Later on January 4, 2011, Mike Halsall, MIT Senior Network & Information Security Analyst, turned over to Secret Service S/A Michael Pickett “historical network flow data concerning 18.55.6.240 & 7.240 [the IP addresses associated with the earlier JSTOR downloads]<sup>6</sup> dating from 12/14 until present and relevant DHCP log information<sup>7</sup> from prior occurrences of ghost-macbook and ghost-laptop [the two guest registrations at issue] JSTOR downloading incidents (from Sept. and Oct.).” Timeline at 7. The disclosure took place only after the MIT General Counsel’s Office approved the disclosure of the information to law enforcement authorities even in the absence of a warrant or court order or subpoena – and at a time when MIT personnel were acting as government agents – and in contravention of MIT policy that such information, which exceeded that found in bank records or telephone toll records, would be disclosed only upon the receipt of lawful court orders or subpoenas, *i.e.*, process complying with the Stored Communications Act, 18 U.S.C. §2701 *et seq.* See Section IV, *infra*. In a separate email from Halsall to S/A Pickett on January 8, 2011, Halsall told Pickett that he “hop[ed] to have the pcap/flows/videos/logs all in by to me Monday,

---

<sup>5</sup> See Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law.

<sup>6</sup> Network flow data shows connections made between computers and the amount of information transmitted. It shows the start and stop time of a connection, the source IP address, the IP address of the website contacted, source and destination port numbers, and the number of bytes of information transmitted.

<sup>7</sup> “DHCP” stands for Dynamic Host Configuration Protocol. DHCP assists with the assignment of IP addresses to computers on networks. When a computer joins a network, the computer issues a DHCP request on the network, which asks a DHCP server on the network to provide an IP address to the requesting computer. Part of the information contained in this request is the MAC (Media Access Control) address which is a unique identifier of the network card contained in the computer requesting an IP address. It also includes the commands made by the computer in question. See page 7, *infra*.

possibly sooner – if you don’t already have a copy of the video or pcap [packet capture], I’ll make sure you get one.” Exhibit 2. No warrant or court order has been provided to counsel which would evidence the government’s having, even post-interception, acquired the contents of the warrantless interceptions by seeking judicial authorization as required.

## **II. MIT’S ACTIONS VIOLATED TITLE III.**

### **A. Swartz Had a Reasonable Expectation of Privacy in his Electronic Communications to and from his Netbook.<sup>8</sup>**

Swartz had a subjective expectation of privacy in electronic communications to and from his netbook, and that expectation is one which society should recognize as objectively reasonable. The netbook was connected to the MIT network, but “the mere act of accessing a network does not in itself extinguish privacy expectations.” *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007). MIT has a liberal guest access policy, which was described by Tim McGovern, MIT Manager of Network Security & Support Services, as follows:

No authentication of visitors. Visitor network access is provided as an on-demand self-service process for anyone who walks onto campus, plugs in, or elects to use our wireless network, and declares themselves a visitor, and they get 14 days of network privileges.

No identity verification. Visitors are asked to provide an email address. The email address is not used to verify that a bona fide identity exists . . . .

No authentication of users accessing JSTOR.org. By agreement, JSTOR.org allows any computer with a net 18 IP address [an MIT IP address] to access their resources without further identification or authentication.

Exhibit 3. In fact, in internal emails, JSTOR described MIT as “unique” in having an open campus.

Exhibit 4. Unlike other institutions which require passwords to access their servers and require additional layers of authentication to access digital libraries such as JSTOR, MIT required neither

---

<sup>8</sup> Swartz incorporates by reference the discussion in Section II of his Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law.

a password, a formal affiliation with the school, or any form of identification for any visitor to become an authorized guest enjoying access to the MIT electronic communication service which was the equal of that afforded to MIT students and professors.

Swartz was validly signed on to the MIT network as a guest, as the MIT guest policy permitted him to be, as verified by an October 14, 2010, email from Ellen Duranceau, MIT Program Manager of Scholarly Publishing and Licensing, to Brian Larsen at JSTOR, informing him that “[o]ur investigations here point to the same *guest* that was involved in the 9/27 incident. We don’t have enough information to follow the trail completely, but the signs suggest that the same *guest user* was responsible for this latest activity. . . . all of this excessive use was caused by a *guest visitor* at MIT,” Exhibit 5 (emphasis added), and then by an October 18, 2010, email from Ms. Duranceau to Tim McGovern, MIT Manager of Network Security & Support Services:

Tim and Mike:

Would it be accurate for me to answer [JSTOR’s] query this way:

*“We offer guests access to the MIT network, and this practice will continue. However, once we [in the future] institute our additional authorization layer for JSTOR, this route will be closed to guests. So we will have closed the pathway used.”*

\* \* \* \*

Mike, I will be asking JSTOR about your mod\_rewrite idea once I check in with Rich Wenger in the Libraries and once JSTOR has shifted more clearly into implementing the new method rather than still working on resolving the excessive use issue.

Exhibit 6 (emphasis added). Thus, MIT had an open-access network that permitted anyone to access it by signing in as a visitor/guest, and anyone signed in to the MIT network was permitted to access JSTOR without further identification or authorization. The name and email address used to sign in as a visitor were fundamentally irrelevant to MIT, as it did not use it in any way to identify the visitor or even to ascertain whether it was a “bona fide identity,” nor did guests to the MIT network receive notice that they were prohibited from using static IP addresses, changing IP addresses, or changing MAC addresses when accessing the MIT network on successive occasions. Neither MIT nor JSTOR

initiated the additional authorization protocol prior to the seizure of the netbook and Swartz's arrest on January 6, 2011.

That MIT regarded Swartz as a guest user is also confirmed by several other MIT communications during the fall of 2010. On September 29, 2010, Ellen Duranceau informed Brian Larsen at JSTOR that "the origin of the activity was *a guest visiting MIT*." Exhibit 7 (emphasis added). JSTOR is available to "[u]sers [who] come to MIT to establish a guest account on the network, and "do not have to have MIT affiliation to use the content." Summary of Key Points by Ellen Duranceau, Exhibit 8. *See* Email from Ellen Duranceau to Ann Wolpert, October 15, 2010, Exhibit 9 ("we cannot identify the *guest* involved in these incidents" (emphasis added)); Email from Ellen Duranceau to Brian Larsen, October 15, 2010, Exhibit 10 ("[o]ur records and logs . . . do not allow us to definitively identify the *guest*" (emphasis added)); Email from Ellen Duranceau to Rich Wenger, October 18, 2010, Exhibit 11 ("it appears that the individual used MIT's wireless network guest account process").

In addition, MIT's written policy on DHCP logs created a reasonable expectation of privacy in *that* information, providing that they would be deleted after 30 days, IS&T Policies:DHCP Usage Logs Policy, available at <http://ist.mit.edu/about/policies/dhcp-usage-logs> (last visited September 24, 2012), and that they would be disclosed *only* in response to a court order or subpoena:

When any network device, e.g., a computer, connects to MITnet and is assigned a dynamic IP address, MIT's DHCP server adds a record to its log containing the following information:

- The date and time of the request
- The MAC address of the requesting device or computer
- The IP address provided
- The specific DHCP command that was issued
- Other technical information related to the request

In the event of a request relating to a potential legal proceeding, IS&T staff may create a case in Request Tracker and store subsets of a log pertinent to the case at hand in the case record.

The DHCP server is in a secure location and complies with secure data storage best practices. IS&T's Network Services Infrastructure team acts as the data custodian for DHCP logs, and ensures that the logs are stored securely and are deleted when they expire.

\* \* \* \*

*MIT is required to comply with a court order or valid subpoena that requests the disclosure of information contained in DHCP logs. Failure to comply could have serious consequences for the individuals, IS&T, and the Institute. MIT's Office of the General Counsel is qualified and authorized to confirm that a request for information contained in logs is legitimate and not an improper attempt to gain access to confidential information.*

*Id.* (emphasis added).

Moreover, on many occasions, the MIT RADIUS log server provided further evidence documenting MIT's authorization of Swartz's access to the MIT network:

**Remote Authentication Dial In User Service (RADIUS)** is a networking protocol that provides centralized Authentication, *Authorization*, and Accounting (AAA) management for computers to connect and use a network service. . . . Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services. . . . The RADIUS server is usually a background process running on a UNIX or Microsoft Windows server. RADIUS serves three functions:

- to authenticate users or devices before granting them access to a network,
- *to authorize those users or devices for certain network services* and
- to account for usage of those services.

<http://en.wikipedia.org/wiki/RADIUS> (last visited September 23, 2012)(emphasis added). Swartz, accordingly, maintained a reasonable expectation of privacy in the communications to and from his netbook and that expectation was objectively reasonable.

**B. MIT's Actions in Intercepting Communications to and from Swartz's Netbook and Disclosure of the Intercepted Communications Violated Title III.**

18 U.S.C. §2511(1) prohibits:

(a) intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

\* \* \* \*

(c) intentionally disclos[ing], or endeavor[ing] to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the

information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally us[ing], or endeavor[ing] to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . . .

18 U.S.C. §2510(12) defines “electronic communication” as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce . . . .” Section 2510(4) defines “intercept” as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” “Contents” is in turn defined as “*any* information concerning the substance, purport or meaning” of the communication. §2510(8)(emphasis added).

The packet capture, which targeted the content of data being sent to or from the netbook that was discovered in Building 16's data room, revealed the contents of electronic communications of all electronic communications intercepted. *See* Email from Dave Newman, MIT Senior Network Engineer, to S/A Pickett, January 5, 2011, Exhibit 12 (“I have collected about 70G of network traffic so far with about 98% of which is the JSTOR journal downloads”). Use of the packet capture constituted the interception of electronic communications of the defendant and others, including, but not limited to, those with whom he was communicating within the meaning of Title III, *see, e.g., United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005)(*en banc*)(diverting incoming communications constitutes interception within the meaning of Title III), which was unlawful in the absence of a valid Title III order authorizing the interceptions of the electronic communications, of which none were sought or issued here.



The DHCP logs also captured content as they captured the message sent from the sending computer requesting an IP address, which is the “substance, purport, or meaning” of the communication.<sup>9</sup> The network flow data showed that a communication took place between one computer and another and the amount of information transmitted. These, too, constitute “contents.”<sup>10</sup> In *In re Application of United States*, 396 F.Supp.2d 45, 48-49 (D.Mass. 2005), the Court recognized that “dialing, routing, addressing and signaling information” may disclose “content” and mandated that the order include instructions to the provider that “[t]he disclosure of the ‘contents’ of communications is prohibited pursuant to this Order even if what is disclosed is also dialing, routing, addressing and signaling information” and that “the term ‘contents’ of communications includes subject lines, application commands, search queries, requested file names, and file paths.” *See, e.g., United States v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008)(suggesting that a technique which reveals the URL visited would be “constitutionally problematic”).

Therefore, the interceptions were unlawful unless they fell within an exception to the prohibitions of §2511. The “provider exception” to Title III, §2511(2)(a)(i) provides:

It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose or use that communication in the normal course of his employment while engaged in any activity which is a *necessary incident to the rendition of his service or to the protection of the rights and property of the provider of that service . . .*

---

<sup>9</sup> Another issue specific to the DHCP logs is addressed in Section III, *infra*.

<sup>10</sup> Such information is not analogous to a pen register, which has been held not to reveal content, because a pen register does not even show whether a communication even took place, *see United States v. New York Tel. Co.*, 434 U.S. 159, 167 (1977). Even a pen register requires a court order based upon a “certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.” 18 U.S.C. §3122(b)(2).

(emphasis added).<sup>11</sup> “The statute’s use of the word necessary, its proviso restricting random monitoring and Congress’ intent to maximize the protection of privacy . . . suggests that this authorization should be limited in scope.” *United States v. Freeman*, 524 F.2d 337, 341 (7th Cir. 1975). *See, e.g., United States v. Cornfeld*, 563 F.2d 967, 970 (9th Cir. 1977)(“the authority to intercept and disclose . . . communications is not unlimited”); *United States v. Harvey*, 540 F.2d 1345, 1350 (8th Cir. 1976)(authority granted by §2511(2)(a)(i) “may be exercised only to the extent necessary for ‘the protection of the rights and property of the carrier’”); *United States v. McLaren*, 957 F.Supp. 215, 218 (M.D.Fla. 1997)(“the court must consider whether the provider of electronic communication service had reasonable cause to suspect that *its* property rights were being abused by a particular subscriber”(emphasis added)).

Here, the circumstances demonstrate that MIT personnel did not intercept the communications at issue to protect *MIT’s* rights or property *as a provider of electronic communication service*. Instead, its concern was initially with the protection of the rights and property of JSTOR and thereafter with assisting law enforcement with discovering the motive and intent of the owner of the netbook and in acquiring evidence that would further the criminal investigation of the individual responsible for the JSTOR downloading. Once the netbook was physically discovered, MIT personnel, aware that its owner would return to retrieve the external hard drive that was attached to the netbook and receiving the downloaded data, installed video surveillance to identify the owner and help in his apprehension. The investigation commenced with a notification from JSTOR regarding excessive downloads of journal articles, and thereafter MIT

---

<sup>11</sup> 18 U.S.C. §2510(15) defines “electronic communication service” as “any service which provides to users thereof the ability to send or receive wire or electronic communications.”

personnel worked with JSTOR to develop and institute a plan which would prevent MIT guest users from accessing JSTOR without an additional level of authorization and permission. There was no need for further investigation on MIT's part, as its electronic communication system was never in the slightest danger of injury or other detrimental impact. Once the netbook was located, MIT advised JSTOR of the discovery and asked it to block the particular IP address it was using. *See* Exhibit 13. MIT also had the option, which it did not choose to exercise, to simply take the netbook offline. Instead, it kept the connection alive only to assist law enforcement and to further a criminal investigation, objectives well outside the narrow parameters of the provider exception to the general prohibition of warrantless interceptions of wireless communications in transit..

Even at the outset of the investigation which began again on January 3, 2011, the objective was to placate JSTOR, which had deemed MIT's prior efforts to identify the person responsible for the downloads "tepid," Exhibit 14, and ensure continued MIT access to JSTOR, as witness the central role played in the investigation by Ellen Duranceau, MIT Program Manager of Scholarly Publishing and Licensing, and not a "necessary incident" to the "protection of the rights and property" of MIT as electronic communications service provider. As of the next morning, January 4, 2011, MIT personnel were acting as agents of law enforcement, and their purpose was not to protect MIT's electronic communications system but instead to further the criminal investigation.<sup>12</sup> Section 2511(2)(a)(i) does not extend to the protection of institutional interests in general but instead only to the protection of the electronic communication system itself.<sup>13</sup> Once the ACER was located

---

<sup>12</sup> *See* Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law.

<sup>13</sup> The interceptions also did not fall within the "trespasser exception," §2511(2)(i), because Swartz was not a trespasser, *see* Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law at 16-19, and, most importantly for present purposes, MIT personnel were not, until law enforcement agents

on the morning of January 4, 2011, MIT's problem with JSTOR could have been ended by disconnecting that computer from the MIT network. Instead, it elected to intercept communications, not to protect the MIT system, but to gather information for law enforcement purposes, such as the motive and intent of the person responsible for the downloads, and to determine whether any of the downloaded information had been transmitted to others by the netbook, a purpose which was protective of JSTOR and in furtherance of law enforcement's acquisition of proof of the possible commission of various federal offenses, but not protective of MIT's electronic communication services, as required by the statutory exception.

Moreover, even if the Court were to conclude that MIT, as electronic communications service provider, was acting to protect its own interest *qua* service provider as it searched for the "offending" computer, "the federal courts . . . have construed [§2511(2)(a)(i)] to impose a standard of reasonableness upon the investigating communication carrier." *United States v. Harvey*, 540 F.2d 1345, 1351 (8th Cir. 1976). *See, e.g., United States v. Hudson*, 2011 WL 4727811 at \*7 -\*8 (E.D.La. Oct. 5, 2011) ("The Fifth Circuit has held that this provision imposes a reasonableness requirement on carriers," *citing United States v. Clegg*, 509 F.2d 605, 613-14 (5th Cir. 1975)); *United States v. McLaren*, 957 F.Supp. 215, 218 (M.D.Fla. 1997) (court "must consider whether the interception activities were reasonable"). The interceptions at issue here went far beyond anything that was necessary to the protection of MIT's rights and property; prior to the January 4, 2011, interceptions and the warrantless disclosures of protected information, the ACER laptop had been discovered, its connection to the MIT network had been identified, video surveillance had been instituted to identify the owner, and a narrow shutdown of service to that computer would have accomplished any legitimate goal of protecting MIT's electronic communication service.

---

encouraged and adopted the ongoing packet capture, acting "under color of law."

Similarly, an electronic communications system provider may disclose to law enforcement *only* those intercepted communications which are a “necessary incident” to the protection of the provider’s property rights. *See, e.g., Clegg*, 509 F.2d at 612-13. *See, e.g., United States v. Auler*, 539 F.2d 642, 646 n.10 (7th Cir. 1976)(“Evidence which is obtained through an unreasonably broad surveillance cannot be legally disclosed to the government, regardless of whether it is offered at trial”). Only those communications of which §2511(2)(a)(i) reasonably permits the interception may be disclosed and admitted as evidence at the trial of a criminal case; “evidence obtained through surveillance beyond the authorization of §2511(2)(a)(i) . . . must be suppressed.” *Id.* at 646. None of the disclosures on January 4, 2011, was justified by this narrow exception to an MIT guest’s entitlement to the protections of the Fourth Amendment and Title III. As such, consistent with *Councilman*, the network data capture constituted unlawful interceptions of electronic communications in violation of the Fourth Amendment, requiring suppression of the captured information and all evidence derived therefrom.

### **III. THE GOVERNMENT COULD NOT OBTAIN DHCP LOG INFORMATION IN THE ABSENCE OF A WARRANT OR, AT MINIMUM, A §2703(D) ORDER.**

The DHCP log records and stores a variety of data. *See* page 7, *supra*. For present purposes, the critical fact about DHCP addressees is that their recording and storage allows the tracking of an individual through the location of his computer. Where laptops and other portable devices are concerned, that data is comparable to cell site data in that it permits the government to determine an individual’s location and to track his movements as he moves his laptop from place to place. Two types of DHCP data are at issue here: the historical data which the government sought from MIT, and with which MIT provided the government, and the ongoing real-time DHCP data which law enforcement obtained on an ongoing basis after they assumed control of the investigation on January

4, 2011, all of which was sought, and obtained, by the government without a warrant or a court order issued pursuant to §2703(d).

Individuals have a reasonable expectation of privacy in their movements. *See, e.g., In re Application of United States*, 849 F.Supp.2d 526, 538-43 (D.Md. 2011). Moreover, an individual retains a reasonable expectation of privacy in DHCP log information because, as the Third Circuit held in the cell site location context, “a . . . customer has not ‘voluntarily’ shared his information with [a third party] in any meaningful way.” *In re Application of United States*, 620 F.3d 304, 317 (3d Cir. 2010). As Justice Sotomayor explained in her concurring opinion in *United States v. Jones*, 132 S.Ct. 945 (2012):

More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. *E.g., Smith [v. Maryland]*, 442 U.S. [735,] 742 [(1979)] . . . ; *United States v. Miller*, 425 U.S. 435, 443 . . . (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice ALITO notes, some people may find the “tradeoff” of privacy for convenience “worthwhile,” or come to accept this “diminution of privacy” as “inevitable,” . . . and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disintitiled to Fourth Amendment protection. *See Smith*, 442 U.S., at 749 (Marshall, J., dissenting) (“Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes”); see also *Katz [v. United States]*, 389 U.S. [347,] 351-352 [(1967)] (“[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected”).

*Id.* at 957.

As to both historical and “real time” cell site data, courts have been divided regarding whether the government must demonstrate probable cause as required by the Fourth Amendment or whether the lesser showing required under §2703(d) will suffice. *Compare In re Application of the United States*, 2012 WL 3260215 at \*1-\*2 (S.D.Tex. July 30, 2012); *In re Application of the United States*, 809 F.Supp.2d 113, 118-20 (E.D.N.Y.2011); *In re United States*, 747 F.Supp.2d 827, 837-40 (S.D.Tex.2010); *In re Application of United States*, 736 F.Supp.2d 578, 579 (E.D.N.Y.2010)(requiring showing of probable cause), with *In re Application of United States*, 620 F.3d at 313; *In re Application of United States*, 849 F.Supp.2d 177, 179 (D.Mass. 2012); *United States v. Graham*, 846 F.Supp.2d 384, 396 (D.Md. 2012); *United States v. Benford*, 2010 WL 1266507, at \*2-\*3 (N.D.Ind. March 26, 2010); *In re Applications of United States*, 509 F.Supp.2d 76, 80-81 (D.Mass. 2007); *In re Application of United States*, 396 F.Supp.2d 294, 327 (E.D.N.Y. 2005)(§2703(d) order suffices).

Courts are likewise split with respect to the government’s burden to obtain real time cell site data. *Compare In re Application of the United States*, 849 F.Supp.2d 526 (D.Md. 2011); *In re Application of the United States*, 2009 WL 159187 (S.D.N.Y. Jan.13, 2009); *In re Application of the United States*, 497 F.Supp.2d 301 (D.P.R.2007); *In re Application of the United States*, 2006 WL 2871743 (E.D.Wis. Oct. 6, 2006); *In re Application*, 439 F.Supp.2d 456 (D.Md.2006); *In re United States*, 441 F.Supp.2d 816 (S.D.Tex.2006); *In re United States*, 2006 WL 1876847 (N.D.Ind. July 5, 2006); *In re Application of the United States*, 2006 WL 468300 (S.D.N.Y. Feb. 28, 2006); *In re United States*, 416 F.Supp.2d 390 (D.Md.2006); *In re United States*, 415 F.Supp.2d 211 (W.D.N.Y.2006); *In re United States*, 412 F.Supp.2d 947 (E.D.Wis.2006), *aff’d* 2006 WL 2871743 (E.D.Wis. Oct. 6, 2006); *In re United States*, 407 F.Supp.2d 134 (D.D.C.2006)(requiring a showing of probable cause), with *In re Application of the United States*, 2008 WL 5255815 (E.D.N.Y.

Dec.16, 2008); *In re United States*, 2008 WL 5082506 (E.D.N.Y. Nov. 26, 2008); *In re Application of the United States*, 460 F.Supp.2d 448 (S.D.N.Y.2006); *In re United States*, 433 F.Supp.2d 804 (S.D.Tex.2006); *In re Application of the United States*, 415 F.Supp.2d 663 (S.D.W.Va.2006); *In re Application of the United States*, 411 F.Supp.2d 678 (W.D.La.2006)(probable cause not required).

The cases requiring a showing of probable cause for both historical cell site data and real time cell site data are the better reasoned and more consonant with the requirements of the Fourth Amendment and its historical role in protecting citizens from serious invasions of personal privacy. The same analysis is applicable to both historical DHCP data and real time DHCP data, and the government's acquisition of this information in the absence of a warrant based on probable cause violated the Fourth Amendment. The invasion of this information also has serious First Amendment implications in that it traces an individual's communicational associations. *See In re Application of United States*, 849 F.Supp.2d at 538 n.5. At a minimum, a §2703(d) order was required. Accordingly, the DHCP log information, and all information derived therefrom, including the laptop and hard drive seized from the MIT Student Center which were discovered as an unattenuated result of the "real time" inspection of DHCP logs on January 6, 2011, must be suppressed.

#### **IV. MIT'S ACTIONS VIOLATED THE STORED COMMUNICATIONS ACT ("SCA").**

18 U.S.C. §2702(a)(1) prohibits any person or entity "providing an electronic communication service to the public" from "knowingly divul[ging] to any person or entity the contents of a communication while in electronic storage by that service."<sup>14</sup> Section 2702(a)(3) prohibits "a provider of . . . electronic communication service to the public" from "divul[ging] a record or other

---

<sup>14</sup> "Electronic storage" includes "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic service communication provider for purposes of backup protection of such communication." 18 U.S.C. §2510(17).



information pertaining to a subscriber or a customer of such service . . . .” MIT was a provider of electronic communication service to the public because it freely allowed guests with no affiliation to MIT to access the MIT network and because it provided wireless service which was readily accessible to anyone within reach of its signal, which extended to areas outside the bounds of the MIT campus.<sup>15</sup> As a guest, Swartz was a customer or subscriber of MIT’s electronic communication service. The SCA contains a provider exception similar to that of Title III: the provider of electronic communication service may disclose the content of communications or information pertaining to a subscriber or customer “as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service.” §§2702(b)(5), (c)(3). This exception does not apply for the same reasons previously addressed in conjunction with the provider exception of Title III.

Moreover, here, MIT did not voluntarily disclose the information on its own initiative. Indeed, disclosure of the information was contrary to MIT policy, which provided its users, including guests, with a reasonable expectation of privacy in the DHCP logs and other information collected by MIT. *See* pages 7-8, *supra*. MIT disclosed the information only after its General Counsel’s office authorized the disclosure, *which had been requested by the government after it had assumed control of the investigation and after MIT had deferred to the government’s control over the investigation*. Thus, at the time of the disclosures, MIT personnel were acting as government agents. In short, MIT personnel, by the late morning of January 4, 2011, were acting as agents of federal and state law enforcement.

Congress passed the Stored Communications Act in 1986 as part of the Electronic Communications Privacy Act. “The SCA was enacted because the advent of the Internet

---

<sup>15</sup> MIT’s wireless network signal is available outside of the campus, for example, at the Kendall Hotel and on the streets and sidewalks that border the campus.

presented a host of potential privacy breaches that the Fourth Amendment does not address.” *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 900 (9th Cir.2008)[, *rev’d on other grounds sub nom. City of Ontario v. Quon*, 130 S.Ct 1531 (2010)] (citing Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1209–13 (2004)). The SCA prevents “providers” of communication services from divulging private communications to certain entities and individuals. Kerr, *supra*, at 1213. It “creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information.” *Id.* at 1212. First, the statute limits the government's right to compel providers to disclose information in their possession about their customers and subscribers. 18 U.S.C. § 2703. . . . Second, the statute limits the right of an Internet Service Provider (“ISP”) to disclose information about customers and subscribers to the government voluntarily. 18 U.S.C. § 2702.

*Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d 965, 971-72 (C.D. Cal. 2010).

As addressed in the previous section, MIT could not voluntarily disclose the information without violating the SCA. Under §2703, the government could not lawfully request or obtain access to the content of electronic communications in the absence of a warrant issued in accordance with the Rules of Criminal Procedure. 18 U.S.C. §2703(a).

In passing the Electronic Communications Privacy Act in 1986, Congress expressed the need to expand the protections of the Fourth Amendment to new forms of communication and data storage. 132 Cong. Rec. H4039-01 (1986); S.Rep. No. 99-541, at 1-2 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3555-56. The legislative history indicates that Congress wished to encourage the development and use of these new methods of communication by ensuring that they were protected and private. S.Rep. No. 99-541, at 5. Congress recognized that courts had struggled with the application of the Fourth Amendment to the seizure of intangibles, like telephone conversations. *Id.* at 2. They therefore sought to strike a balance between the competing interests addressed by the Fourth Amendment in the world of electronic communications by “protect[ing] privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs.” *Id.* at 3.

It is clear that Congress wished to apply the protections associated with search warrants to searches authorized under § 2703(a).

*In re United States*, 665 F.Supp.2d 1210, 1220 (D.Or. 2009). The government could not lawfully obtain “record[s] or other information pertaining to a subscriber or customer” of MIT’s electronic communications system in the absence of a warrant or a court order issued pursuant to §2703(d). 18 U.S.C. §2703(c)(1). Under §2703(c)(2), the government may obtain the name and address of a

customer or subscriber, records of session times and duration, length of services and types of service used, and “other subscriber number or identity, including any temporarily assigned network address” only through an administrative, grand jury, or trial subpoena. The information at issue here went beyond this narrow description, but, in any event, the government did not seek the information pursuant to subpoena. The DHCP logs, the network flow data, and the packet capture all either contained “content” of the electronic communications to and from the netbook, in which Swartz had a reasonable expectation of privacy or “record[s] or other information” pertaining to Swartz’s use of MIT’s electronic communications system, in which he also had a reasonable expectation of privacy. Indeed, MIT’s DHCP log policy created an objectively reasonable expectation that those logs would remain confidential unless they were required to be disclosed pursuant to a lawful order or subpoena, of which there was none here. The government’s conduct, in seeking the production of this material without a warrant and without a §2703(d) order violated the Fourth Amendment. *See, e.g., United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). The material at issue must, accordingly, be suppressed, along with all derivative fruits thereof.

Respectfully submitted,  
By his attorney,

**/s/ Martin G. Weinberg**  
Martin G. Weinberg  
20 Park Plaza, Suite 1000  
Boston, MA 02116  
(617) 227-3700 (tel.)  
(617) 338-9538 (fax)  
owlmgw@att.net

**CERTIFICATE OF SERVICE**

I, Martin G. Weinberg, hereby certify that on this 5th day of October, 2012, a copy of the foregoing document has been served via the Court's ECF system on all registered participants, including Stephen P. Heymann, AUSA. One copy of the exhibits to the motion was served on the government by hand this same date.

**/s/ Martin G. Weinberg**

Martin G. Weinberg

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

_____	)	
UNITED STATES	)	
	)	
v.	)	No. 11-10260-NMG
	)	
AARON SWARTZ	)	
_____	)	

**MOTION TO SUPPRESS ALL FRUITS OF WARRANTLESS SEARCHES  
CONDUCTED FROM JANUARY 4, 2011, TO JANUARY 6, 2011,  
AND INCORPORATED MEMORANDUM OF LAW  
(MOTION TO SUPPRESS NO. 2)**

Now comes the defendant Aaron Swartz and respectfully moves that this Honorable Court suppress as evidence at the trial of this case all evidence derived from unlawful warrantless searches of, and unlawful interceptions of electronic communications/data to and from, an ACER netbook belonging to him, from January 4, 2011, through January 6, 2011, and all derivative fruits thereof.

As reason therefor, defendant states:

1. He had a reasonable expectation of privacy in his netbook and in the communications/data flowing to and from it.<sup>1</sup>

2. From January 4, 2011, through January 6, 2011, MIT personnel, Secret Service agents, and Cambridge police unlawfully searched his ACER netbook and intercepted communications/data flowing to and from the netbook, without either a search warrant or an order authorizing the interception of electronic communications under Title III.

3. To the extent that such searches/interceptions were carried out by MIT personnel, they were acting as government agents, and the requirements of the Fourth Amendment apply.

---

<sup>1</sup> All averments herein regarding Swartz's ownership and possession of the ACER laptop and the hard drive are made pursuant to the protections provided by *Simmons v. United States*, 390 U.S. 377, 392-94 (1968).

4. The evidence, along with all derivative fruits thereof, must, therefore, be suppressed.

**THE DEFENDANT REQUESTS A HEARING ON THE WITHIN MOTION.**

**LOCAL RULE 7.1(A)(2) STATEMENT**

The undersigned counsel has conferred with AUSA Stephen Heymann. The government opposes the suppression remedies sought and will respond to defendant's request for a hearing in its response to the motion.

**MEMORANDUM OF LAW**

**I. FACTUAL BACKGROUND.**

From September 27, 2010, until January 4, 2011, MIT personnel conducted an investigation into the downloading of large quantities of material from JSTOR, an online archive which provides access to academic journals.<sup>2</sup> Timeline of events related to JSTOR downloading incident: 9/26/10-1/6/11 ("Timeline"), Exhibit 1 at 1-5. On January 4, 2011, Dave Newman, MIT Senior Network Engineer, located an ACER netbook in a data room in the basement of an MIT building, which Newman believed was the computer being used to download journal articles from JSTOR. Timeline at 6. Newman, in consultation with Paul Acosta, MIT Manager of Network Operations, decided to leave the netbook physically undisturbed and instead to institute a "capture" of the network traffic to and from the netbook, which was done via Newman's laptop, which was connected to the netbook and which intercepted communications coming to it. *Id.*; US Secret Service Investigative Report ("Investigative Report"), Exhibit 15 at 2. These interceptions were commenced without a warrant or other judicial process. At 11:00 am, Captain Jay Perault of the MIT police arrived, along with

---

<sup>2</sup> The events which occurred during this time period are further addressed in a separate motion to suppress. *See* Motion to Suppress All Fruits of Interceptions and Disclosures of Electronic Communications and Other Information by MIT Personnel in Violation of the Fourth Amendment and the Stored Communications Act and Incorporated Memorandum of Law. The events relevant to this motion began on the morning of January 4, 2011.

Det. Joseph Murphy of the Cambridge Police Department and Secret Service S/A Michael Pickett, who told MIT personnel that he handled computer forensics for the Secret Service. *Id.*; Investigative Report at 1. It was decided, “*at the recommendation of Michael Pickett,*” that the netbook would be left in place, with MIT continuing to monitor the traffic to and from it, and that video surveillance would be set up in the data room to assist in identifying “the suspect.” Timeline at 6 (emphasis added). *See* Grand Jury Testimony of Det. Joseph Murphy, July 14, 2011, Exhibit 16 at 66 (“Murphy Grand Jury”)(Murphy testified that after learning that MIT had begun the packet capture, “we” told MIT personnel that “[w]e’d like you to keep this running” and, ultimately, “we end up persuading them to leave that on the system”); Email from Ellen Duranceau, MIT Program Manager of Scholarly Publishing and Licensing, to Ann Wolpert, MIT Director of Libraries, January 4, 2011, 3:35 pm, Exhibit 17 (“the offending computer has been found, on the MIT campus. *The police would like to leave it up and running for a couple of days while the investigation continues*” (emphasis added)). Neither S/A Pickett nor Det. Murphy applied for or received a Title III warrant authorizing the interception of electronic communications or were in any way authorized by judicial process to direct and persuade MIT personnel to intercept communications and other data flowing to and from the ACER netbook between 11:00 am on January 4, 2011, and the time of the seizure of the ACER on January 6, 2011.

During the morning of January 4, 2011, the search participants observed that “the netbook [was] still reaching out to JSTOR and downloading journals.” *Id.* A warrantless NMap search<sup>3</sup> of the netbook showed that ports 22 and 8092 – ports associated with remote access – were open. Timeline at 7; Investigative Report at 1. The laptop was also physically manipulated and

---

<sup>3</sup> NMap is a sophisticated port-scanning software that can determine a large amount of information about a computer, including which of a computer’s ports are open, the computer’s operating system, and which of thousands of services and protocols the computer is using. *See* <http://en.wikipedia.org/wiki/Nmap> (last visited Sept. 19, 2012).

fingerprinted without a warrant by law enforcement officers. The outside of the netbook was examined, including picking it up and manipulating it. *See* Exhibit 18. The netbook was opened, and the computer screen which showed the operating system being used and the log-in screen which showed a computer name of “ghost-laptop” with the user name “Gene Host” were accessed and photographed. *See* Exhibit 19. The log-in screen required a password, and all efforts to bypass it were unsuccessful. Email from S/A Pickett to AUSA Adam Bookbinder, January 5, 2011 (“Pickett 1/5/11 email”), Exhibit 20 at 1. In addition, the closed, hard-shell case containing the hard drive was fingerprinted; the case was opened, and the hard drive, which law enforcement believed was being used to store the downloaded data, was examined and separately finger printed. *See* Exhibit 21. The opening of the hard drive case and examination of the case and its contents were all done by law enforcement officers on January 4, 2011, without a warrant or any other judicial process.

Newman, Acosta, and S/A Pickett, along with Mike Halsall, MIT Senior Network & Information Security Analyst, continued to physically monitor the netbook until 2:30 pm. Timeline at 7. During that time “strategy [was] determined for continual monitoring of traffic to/from the netbook.” *Id.* After the MIT General Counsel’s office approved the disclosure of information to law enforcement agents even in the absence of a warrant or process complying with the Stored Communications Act (“SCA”), 18 U.S.C. § 2701 *et seq.* (and in contravention of MIT’s published policies of only disclosing such information after receipt of such process), and at a time when MIT personnel were acting as government agents, Halsall gave S/A Pickett historical network flow data relating to two IP addresses associated with the netbook from December 14, 2010, up to that date,<sup>4</sup> and DHCP log information for computers using the MIT network as “ghost macbook” and “ghost

---

<sup>4</sup> Network flow data shows connections made between computers and the amount of information transmitted. It shows the start and stop time of a connection, the source IP address, the IP address of the website contacted, source and destination port numbers, and the number of bytes of information transmitted.



laptop” for time periods including September and October of the previous year. *Id.*; Investigative Report at 3.<sup>5</sup> The scene was “restored to the way it was found.” Timeline at 7. At 3:50 pm on January 4, 2011, Ellen Duranceau sent an email to Brian Larsen at JSTOR stating that she had “just had an update from Mike Halsall of our network security team. *The investigation has moved beyond MIT and is now being handled by law enforcement*, including federal law enforcement . . . . The machine through which the abuse occurred is still live, pending further steps in the investigation.” Exhibit 22 (emphasis added). At 3:26 pm, an individual, later identified as Swartz, was observed via the video surveillance to enter the data room and replace the external hard drive attached to the netbook with a different one. Timeline at 7.

S/A Pickett left the MIT campus at 4 pm on January 4, and Newman waited to hear from him regarding “where to put the captured network traffic.” Timeline at 7. Thereafter, Pickett contacted the CERT Coordination Center at the Software Engineering Institute at Carnegie Mellon University<sup>6</sup> and received instructions regarding how to upload the network flow and DHCP log data to the CERT drop box. Investigative Report at 3. S/A Pickett authored an email at 6:46 pm on January 4, 2011, stating that “[t]he flow traffic is currently being uploaded to the CERT dropbox.” Exhibit 23.

On January 5, 2011, Ellen Finnie Duranceau, MIT Program Manager of Scholarly Publishing and Licensing, took notes of a conversation with Halsall in which she indicated that the netbook was “left in place to capture traffic” because law enforcement “want[ed] to find intent + motive.” Exhibit

---

<sup>5</sup> “DHCP” stands for Dynamic Host Configuration Protocol. DHCP assists with the assignment of IP addresses to computers on networks. When a computer joins a network, the computer issues a DHCP request on the network, which asks a DHCP server on the network to provide an IP address to the requesting computer. Part of the information contained in this request is the MAC (Media Access Control) address which is a unique identifier of the network card contained in the computer requesting an IP address. The DHCP logs provide, therefore, significant information in addition to simply the IP addressed used by the computer in question.

<sup>6</sup> CERT has a longstanding and ongoing relationship with the Department of Justice, including the Secret Service, providing technological support for DOJ criminal investigations.

24 at 2. Those same notes stated that it was “now a Federal case” and that everything that had been provided was done “by choice,” and not pursuant to a subpoena. *Id.* at 3. Also on January 5, 2011, Newman emailed S/A Pickett at 5:02 pm, stating: “I have collected about 70G of network traffic so far with about 98% of which is the JSTOR journal downloads. . . *I was just wondering what the next step is.*” Exhibit 25 (“Email chain”) at 2 (emphasis added).<sup>7</sup> The next morning, January 6, 2011, at 9:37 am, Perault sent an email to Newman, S/A Pickett, and Det. Murphy suggesting that the netbook and hard drive be taken offline and asking if the hard drive should be “printed,” *i.e.*, imaged. *Id.* S/A Pickett responded, agreeing that the netbook should be taken offline and imaged. *Id.* However, he recommended that the video surveillance be maintained because he believed that whoever was using it would return once he noticed that the netbook was offline. Email chain at 1. There was no consideration in any email or report of seeking a judicial warrant for the ongoing interceptions of communications that were being diverted onto and copied on Newman’s computer or any consideration of whether judicial process was required for the real-time monitoring of MIT’s DHCP logs to identify whether and when the ACER netbook was moved or its connection to the MIT network altered. Given the ongoing video surveillance of the laptop – and the known practice of the owner to return to the data room to swap external hard drives – it cannot be contended that the purpose of the ongoing interceptions of data or the decisions to image the ACER were made to identify the owner rather than for purely law enforcement purposes.

At 12:32 pm on January 6, 2011, an individual later identified as Swartz was observed via video surveillance to enter the data room, remove the netbook and hard drive, and place them in his backpack. Timeline at 7; Investigative Report at 3. Swartz was arrested shortly thereafter; his

---

<sup>7</sup> The network traffic being intercepted and copied without a warrant was the content of the data or emails or communications between the ACER netbook and third parties, including, but not limited to, JSTOR.

backpack was searched, but the netbook was not there. Investigative Report at 3. When Halsall checked the DHCP logs for computer registrations using the word “ghost” later that afternoon, he observed that the netbook was still active on the MIT network using the same MAC address it had used on January 4, 2011. The netbook was traced to the fifth floor of the Student Center. S/A Pickett was notified and met Halsall at the Student Center. They located the netbook and external hard drive neatly placed under a table, connected to the MIT network. S/A Pickett examined the netbook, which appeared to be frozen halfway in the shutdown state. Attempts were made by the Secret Service to access a terminal on the machine but were unsuccessful; “[i]t was determined it would not be possible to conduct live forensics or capture a snapshot of the memory of the computer in its current state.” Investigative Report at 3. The laptop and hard drive were again fingerprinted on January 6, 2012. The laptop and hard drive were then seized and turned over to MIT police. Timeline at 10; Investigative Report at 3. In a January 8, 2011, email from Halsall to Mark Sillis, Halsall’s supervisor, discussing Swartz’s movements on January 6, 2011, Halsall stated that he had been “gathering up all the stuff for Pickett.” Exhibit 26. In a separate email from Halsall to S/A Pickett on January 8, 2011, Halsall told Pickett that he “hop[ed] to have the pcap/flows/videos/logs all in by to me Monday, possibly sooner – if you don’t already have a copy of the video or pcap [packet capture], I’ll make sure you get one.” Exhibit 2.

At no time before or during these events was Title III authorization sought for the interception of electronic communications to or from the netbook. No warrant (not even a “sneak and peek” warrant pursuant to 18 U.S.C. §3103a which would have preserved the secrecy of the ongoing efforts to identify the owner of the netbook) to search the netbook or the external hard drive, both of which were seized on January 6, 2011, was obtained until February 9, 2011. Even then, the warrant was not executed, necessitating a reapplication for a search warrant, which was again issued

on February 24, 2011.

## **II. SWARTZ HAD A REASONABLE EXPECTATION OF PRIVACY IN THE NETBOOK AND EXTERNAL HARD DRIVE.**

“Courts routinely recognize that individuals possess objectively reasonable expectations of privacy in the contents of their computers.” *United States v. Howe*, 2011 WL 2160472 at \*7 (W.D.N.Y. May 27, 2011), adopted 2012 WL 1565708 (W.D.N.Y. May 1, 2012). “Expectations of privacy in the contents of a computer are likened to expectations of privacy in other types of containers, such as suitcases or briefcases. . . . ‘Because intimate information is commonly stored on computers, it seems natural that [personal] computers should fall into the same category as suitcases, footlockers, or other personal items that command a high degree of privacy.’” *United States v. Trejo*, 2010 WL 940036 at \*4 (E.D.Mich. March 12, 2010), *aff’d* 471 Fed. Appx. 442 (6th Cir. 2012), *quoting United States v. v. Andrus*, 483 F.3d 711, 718 (10th Cir. 2007). “Whether a defendant has a reasonable expectation of privacy in a particular place is a two-pronged inquiry. [The Court] consider[s] first, whether the movant has exhibited an actual, subjective, expectation of privacy; and second, whether such subjective expectation is one that society is prepared to recognize as objectively reasonable.” *United States v. Werra*, 638 F.3d 326, 331 (1st Cir. 2011). Both of these requirements are amply satisfied here.

The netbook and hard drive belonged to Swartz, and he took pains to place the netbook and hard drive in locations in which they would be free from interference by outsiders, first in a basement data room which appeared from the outside to be locked, concealed under a box, Timeline at 6; Murphy Grand Jury at 82-83, and then under a table in a private area of the Student Center. Critically, the computer was password protected to prevent access to its contents. *See, e.g., United States v. Reeves*, 2012 WL 1806164 at \*8 (May 17, 2012)(fact that defendant’s computer was password protected was “sufficient to show her intent to exclude members of the public and maintain

privacy in the documents kept on her computer”); *Clements-Jeffrey v. City of Springfield*, 2011 WL 3207363 at \*3 (S.D. Ohio July 27, 2011)(“Personal computers that are password protected are subject to even greater privacy protection”); *United States v. Griswold*, 2011 WL 7473466 at \*12 (W.D.N.Y. June 2, 2011)(“In this age of electronically stored information a reasonably well trained police officer should know that an individual’s use of a password to protect against unauthorized access to electronic files stored on his or her computer is no less an indication of personal privacy than the use of a lock and key by the owner of a file cabinet”); *Howe*, 2011 WL 2160472 at \*7 (defendant’s use of a password to protect the files on the computer demonstrates his subjective expectation of privacy in the contents); *see also Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001)(co-user of computer could not validly consent to search of defendant’s password-protected files on the computer to which co-user did not have access). Swartz plainly had a subjective expectation of privacy in the netbook and the external hard drive.

That expectation, moreover, is one which society should recognize as objectively reasonable. The netbook was connected to the MIT network, but “the mere act of accessing a network does not in itself extinguish privacy expectations.” *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007). MIT has a liberal guest access policy, which was described by Tim McGovern, MIT Manager of Network Security & Support Services, as follows:

No authentication of visitors. Visitor network access is provided as an on-demand self-service process for anyone who walks onto campus, plugs in, or elects to use our wireless network, and declares themselves a visitor, and they get 14 days of network privileges.

No identity verification. Visitors are asked to provide an email address. The email address is not used to verify that a bona fide identity exists . . . .

No authentication of users accessing JSTOR.org. By agreement, JSTOR.org allows any computer with a net 18 IP address [an MIT IP address] to access their resources without further identification or authentication.

Exhibit 3. Nothing on the MIT website relating to guest use of the MIT network diminishes this legitimate expectation of privacy. Nothing on the MIT website precludes guests – or students or

faculty members – from leaving their laptops in private areas of the campus while downloading data from the internet.

Contrary to the government’s argument in its Response to Defendant Aaron Swartz’s Motion for Discovery (Doc. 41) at 6, Swartz did not forfeit his expectation of privacy in his netbook and external hard drive because he was a trespasser; those items remained closed containers which were his personal property and which were not abandoned, *see* pages 11-12, *infra*. Swartz was not a trespasser at MIT in any sense. The MIT campus is not closed to persons other than students, faculty, and employees. On the contrary: it is an open campus with practices that encourage persons who are members of the broader Cambridge technical community to share its resources. Swartz has lectured to an MIT class, audited classes at MIT, worked on projects with MIT professors, and has been a valued member of MIT forums and groups.

The cases on which the government relied are uniformly inapposite. In *United States v. Terry*, 2007 WL 496630 (S.D.Ga. Feb. 12, 2007), *aff’d* 258 Fed. Appx. 304 (11th Cir. 2007), the defendant appropriated to himself a unit in a storage facility which he did not rent and had no right to occupy and affixed a padlock to it. Similarly, in *United States v. Pitt*, 717 F.2d 1334 (11th Cir. 1983), the defendant padlocked a room belonging to his girlfriend’s landlady, to which his girlfriend, as the tenant, had no right of access or use, and which the landlady had reserved to her exclusive use. In *United States v. Hightower*, 1987 WL 44897 (6th Cir. Sept. 28, 1987), the defendant placed locks on country club lockers which he was not authorized to use and for which he had not paid the required fee. In *United States v. Sanchez*, 635 F.2d 47 (2d Cir. 1980), the defendant was unable to demonstrate ownership of or authority from the owner to possess and use the automobile which was the subject of the challenged search. What *Sanchez* says is that “a mere trespasser has no Fourth Amendment protection *in premises* he occupies wrongfully.” *Id.* at 64 (emphasis added). Like the

other cases on which the government relied, *Sanchez* involved an assertion of a reasonable expectation of privacy in the entire premises at issue – the storage unit, the landlady’s storage room, the car, the lockers – which is not the issue here. Swartz does not suggest that he had a reasonable expectation of privacy in the data room, but solely in his private property located therein – the netbook and the external hard drive – and in the electronic communications to and from his netbook. The data room was located within a network of hallways which were used by people to travel between MIT buildings, especially in the winter. Murphy Grand Jury at 82-83. There were classrooms on the same floor, and students used the corridor to attend classes. There were no signs ordering people to keep out, *see* Exhibit 27, and the door to the data room opened readily with a “quick jerk.” Murphy Grand Jury at 84. Swartz simply was not a trespasser in the sense which led to the decisions in *Sanchez* and the government’s other cases. *See United States v. Scott*, 673 F.Supp.2d 331, 339 (M.D.Pa. 2009)(defendant had reasonable expectation of privacy in computer belonging to him seized from apartment where defendant did not contend that he lived or stayed for any period of time or that he was ever invited to the apartment or that he had a key to the apartment).

Nor did Swartz abandon the netbook. To find abandonment, there must be “clear and unequivocal evidence” that the defendant intended to abandon the property. *United States v. Crist*, 627 F.Supp.2d 575, 580-81 (M.D.Pa. 2008)(holding that defendant did not abandon computer where he returned to house to get it 26 days after his rent became overdue, eviction proceedings had not commenced, and defendant had received no notice that his property would be removed), *quoting United States v. v. Fulani*, 368 F.3d 351, 354 (3d Cir. 2008). Here, Swartz neither denied ownership of the netbook nor physically relinquished the item. *See United States v. James*, 353 F.3d 606, 615-16 (8th Cir. 2003)(defendant did not abandon computer disks he gave to a friend to store, even after he told the friend to destroy them); *United States v. Upham*, 168 F.3d 532, 357 (1st Cir.

1999)(defendant did not abandon computer images by deleting them); *United States v. Infante-Ruiz*, 13 F.3d 498, 501-02 (1st Cir. 1994)(defendant did not repudiate privacy interests by leaving his unlocked briefcase in the locked truck of another person's car, even though he allowed other people to store items in it because "he did nothing to indicate its availability to the public generally nor did his actions betray an intention to forego an owner's normal right to exclude those he wished to exclude"). Notably, the law enforcement officials on the scene did not believe that the netbook was abandoned, as they set up video surveillance in anticipation of the owner's return, and, indeed, Swartz was observed returning to the netbook on the afternoon of January 4, 2011, and on January 6, 2011.

The netbook and external hard drive were seized from the Student Information Processing Board Office, a small private office located in the MIT student center, *i.e.*, it was not seized from the Building 16 data closet. A student who was present when Swartz entered the room, and whose identity is known to the government, told Cambridge Police that Swartz asked permission to use a network drop in the room, and the student pointed him to one. After the student told Swartz that he was leaving and needed to lock the room, Swartz left, as did the student, locking the door behind him. Thus, Swartz had the permission of a person with authority over the room (as evidenced by his possession of keys to it) to connect to the MIT network in the room and had every reason to believe that the netbook was in a private, locked space where it would remain unmolested. He had both a subjective and objectively reasonable expectation of privacy in the netbook and hard drive.

### **III. THE SEARCHES AT ISSUE HERE.**

#### **A. The January 4, 2011, and January 6, 2011, External Examination and Fingerprinting of the Netbook and Hard Drive.**

While the netbook and external hard drive were in plain view, and law enforcement officers were lawfully on the premises, the physical manipulation of the netbook and external



hard drive by law enforcement personnel to examine its external attributes and to fingerprint it constituted a warrantless search within the meaning of the Fourth Amendment. *See, e.g., Arizona v. Hicks*, 480 U.S. 321, 324-25 (1987)(officer’s moving of turntable to examine its exterior constituted Fourth Amendment search). As the Supreme Court explained in *Hicks*: “[T]he distinction between ‘looking’ at a suspicious object in plain view and ‘moving’ it even a few inches is much more than trivial for purposes of the Fourth Amendment. It matters not that the search uncovered nothing of any great personal value to respondent – serial numbers rather than (what might conceivably have been hidden behind or under the equipment) letters or photographs. A search is a search, even if it happens to disclose nothing but the bottom of a turntable.” *Id.* at 325. *See, e.g., United States v. Paneto*, 661 F.3d 709, 714 n.3 (1st Cir. 2011)(“Under *Hicks*, it is clear that the Fourth Amendment forbids handling an item to expose something hidden”). The same reasoning applies with equal force to the opening of the hard drive case and the examination of the hard drive contained within it. The fruits of the external examination of the netbook and the external hard drive and its case must, accordingly be suppressed.

#### **B. The Internal Examination of the Netbook.**

The opening of the netbook, the observation of the screen showing the operating system in use and the log-in screen, the attempts to bypass the log-in screen, and the conducting of an NMap search of the netbook to determine which ports were open, constituted a search within the meaning of the Fourth Amendment. *See, e.g., United States v. Musgrove*, 845 F.Supp.2d 932, 949 (E.D.Wis. 2011)(touching key or moving mouse to expose screen that was not previously in view is Fourth Amendment search); *United States v. Crist*, 627 F.Supp.2d 575, 585 (M.D.Pa. 2008)(running of hash values is a Fourth Amendment search); *see also United States v. Phillips*, 477 F.3d 215, 217 (5th Cir. 2007)(describing port scanning as “the

electronic equivalent of ‘rattling doorknobs’ to see if easy access can be gained to a room”). The internal examination of the laptop and its functions was a search, just as opening a locked briefcase or file cabinet and examining its contents is, and could not lawfully be conducted in the absence of a search warrant duly issued upon a showing of probable cause. The fruits of this internal examination must, accordingly, be suppressed.

### **C. The Capture of Electronic Communications to the Netbook.**

18 U.S.C. §2510(12) defines “electronic communication” as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce . . . .” Section 2510(4) defines “intercept” as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” “Contents” is in turn defined as “any information concerning the substance, purport or meaning” of the communication. §2510(8). The “packet capture” which MIT continued to undertake at the recommendation of S/A Pickett and the persuasion of Det. Murphy captured the entire communication, including subject matter and content. That it intercepted the content of electronic communications is obvious from Newman’s January 5, 2011, email to S/A Pickett informing him that he had “collected about 70G of network traffic so far with about 98% of which is the JSTOR journal downloads.” Email chain at 2. Even accepting Newman’s calculations, that means that 2% of the 70G of intercepted data, communications, emails, and the like, involved parties other than JSTOR, *see, e.g.,* Exhibit 28 (showing interception of communications of third party), a significant violation of the Fourth Amendment, as was the warrantless seizure of the 98% of the content emanating, according to Newman, from JSTOR. Obviously, Newman, working in concert with S/A

Pickett, must have searched his copy of the intercepted communications to make his numerical assessment. Use of the packet capture constituted the interception of electronic communications within the meaning of Title III, *see, e.g., United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005)(*en banc*)(diverting incoming communications constitutes interception within the meaning of Title III), which was unlawful in the absence of a valid order authorizing the interceptions of the electronic communications, of which none were sought or issued here.

None of the exceptions to the prohibition of warrantless interception of electronic communications are applicable here. Section 2511(2)(a)(i) provides:

It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights and property of the provider of that service . . . .

This section is inapplicable here because, as more fully addressed in the next section of the memorandum, MIT personnel were acting as government agents beginning no later than 11:00 am on January 4, 2011, and the packet capture was conducted by them as government agents. Because they were acting as government agents, “the requirements of the Fourth Amendment . . . override statutory authority.” *United States v. Pervaz*, 118 F.3d 1, 5 (1st Cir. 1997). *See McClelland v. McGrath*, 31 F.Supp.2d 616, 618 (N.D. Ill. 1998)(“What the officers do not seem to understand . . . is that *they* are not free to ask or direct Cellular One to intercept *any* phone calls or disclose their contents, at least not without complying with the judicial authorization provisions of the Wiretap Act, *regardless* of whether Cellular One would have been entitled to intercept those calls on its own initiative” (emphasis in original)); *United States v. Auler*, 539 F.2d 642, 647 (7th Cir. 1976)(“Government agents must not rely on telephone company employees to act on their behalf

without complying with the requirements of the Fourth Amendment. . . . In no situation may the Government direct the telephone company to intercept wire communications in order to circumvent the warrant requirements of a reasonable search”); *United States v. Hudson*, 2011 WL 4727811 at \*3 (E.D.La. Oct. 5, 2011)(“If the Alltel employees were government agents, . . . they would not satisfy the carrier exception of Title III, and their conduct would be judged under the standards of the Fourth Amendment”).<sup>8</sup>

This conclusion is reflected in the USDOJ manual, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, which instructs that the provider exception “does not permit law enforcement officers to direct or ask system administrators to monitor for law enforcement purposes.” *Id.* at 174-75. The Manual continues:

After law enforcement and the provider have communicated with each other, . . . the cautious approach is only to accept the fruits of a provider’s monitoring if certain criteria have been met that indicate that the provider is monitoring and disclosing to protect its rights or property. These criteria are: . . . (3) *law enforcement has not tasked, directed, requested or coached the monitoring for law enforcement purposes*, and (4) law enforcement does not participate in or control the actual monitoring that occurs.

*Id.* at 175 (emphasis added). Here, law enforcement plainly, at a minimum, “requested or coached the monitoring for law enforcement purposes.” *See* Murphy Grand Jury at 66 (Murphy testified that after learning that MIT had begun the packet capture, “we” told MIT personnel that “[w]e’d like you to keep this running” and, ultimately, “we end up *persuading* them to leave that on the system”(emphasis added)). The provider exception is, accordingly, inapplicable.<sup>9</sup>

---

<sup>8</sup> MIT’s interceptions prior to January 4, 2011, are addressed in a separate motion to suppress. *See* Motion to Suppress All Fruits of Interceptions and Disclosures of Electronic Communications and Other Information by MIT Personnel in Violation of the Fourth Amendment and the Stored Communications Act and Incorporated Memorandum of Law.

<sup>9</sup> Moreover, §2511(2)(a)(i) has a reasonableness requirement – an electronic communications service provider may intercept communications only insofar as such interception is “a necessary incident” to the protection of its rights and property. *See, e.g., United States v. Harvey*, 540 F.2d

The “trespasser” provision is also inapplicable. Section 2511(2)(i) provides:

It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if –

- (I) the owner or operator of the protected computer authorizes the interception of the computer trespasser’s communications on the protected computer;
- (II) the person acting under color of law is lawfully engaged in an investigation;
- (III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser’s communications will be relevant to the investigation; and
- (IV) such interception does not acquire communications other than those transmitted to and from the computer trespasser.

Section 2510(21) defines “computer trespasser” as “a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer.” This provision is inapplicable for three separate reasons. First, Swartz was not a “computer trespasser” within the meaning of Title III because he did not “access a protected computer without authorization.” Quite the contrary – he was validly signed on to the MIT network as a guest, as the MIT guest policy permitted him to be, and, accordingly, maintained a reasonable expectation of privacy in the communications to and from his netbook. That MIT regarded him as a guest user is confirmed by a number of MIT communications during the fall of 2010. On October 14, 2010, Ellen Duranceau, MIT Program Manager of Scholarly Publishing and Licensing, emailed Brian Larsen at JSTOR, informing him that “[o]ur investigations here point to the same *guest* that was involved in the 9/27 incident. We don’t have enough

---

1345, 1351 (8th Cir. 1976); *United States v. Hudson*, 2011 WL 4727811 at \*7 -\*8 (E.D.La. Oct. 5, 2011). The packet capture went far beyond anything was necessary to the protection of MIT’s rights and property. Once the netbook was identified, running, with an external hard drive, it was fully expected that the owner would return, hence the installation of video surveillance to identify the owner. The data capture was not relevant to protecting MIT’s property as an electronic communication system provider.

information to follow the trail completely, but the signs suggest that the same *guest user* was responsible for this latest activity. . . . all of this excessive use was caused by a *guest visitor* at MIT” Exhibit 5 (emphasis added). JSTOR is available to “[u]sers [who] come to MIT to establish a guest account on the network, and “do not have to have MIT affiliation to use the content.” Summary of Key Points by Ellen Duranceau, Exhibit 8. *See* Email from Ellen Duranceau to Ann Wolpert, October 15, 2010, Exhibit 9 (“we cannot identify the *guest* involved in these incidents” (emphasis added)); Email from Ellen Duranceau to Brian Larsen, October 15, 2010, Exhibit 10 (“[o]ur records and logs . . . do not allow us to definitively identify the *guest*” (emphasis added)); Email from Ellen Duranceau to Tim McGovern, October 18, 2010, Exhibit 6 (asking if it would be accurate to say: “We offer guests access to the MIT network, and this practice will continue. However, once we institute our additional authorization layer for JSTOR, this route will be closed to guests”); Email from Ellen Duranceau to Rich Wenger, October 18, 2010, Exhibit 11 (“it appears that the individual used MIT’s wireless network guest account process”). Second, the *content* of the communications was not relevant to the investigation. Third, just as the provider exception cannot override the protections of the Fourth Amendment, neither may the statutory trespasser exception. The Fourth Amendment is fully applicable to these interceptions.

**IV. TO THE EXTENT THAT ANY OF THE SEARCHES AT ISSUE HEREIN WERE PERFORMED BY MIT PERSONNEL RATHER THAN LAW ENFORCEMENT OFFICERS, THE MIT PERSONNEL WERE ACTING AS AGENTS OF THE GOVERNMENT, AND THE FOURTH AMENDMENT IS FULLY APPLICABLE TO THEIR ACTIONS.**

While purely private action is not subject to Fourth Amendment scrutiny, from the point that S/A Pickett and Det. Murphy arrived on the scene, the MIT personnel ceased to be private actors and, instead, acted to further the law enforcement investigation rather than the protection of MIT’s interests. The First Circuit has identified three factors relevant to the determination whether a private individual was acting as a government agent: “the government’s role in instigating or participating

in the search, its intent and the degree of control it exercises over the search and the private party, and the extent to which the private party aims primarily to help the government or to serve its own interests.” *United States v. Pervaz*, 118 F.3d 1, 6 (1st Cir. 1997). *See, e.g., United States v. Hardin*, 539 F.3d 404, 419 (6th Cir. 2008)(“the police must have instigated, encouraged or participated in the search,” and “the individual must have engaged in the search with the intent of assisting the police in their investigative efforts”); *United States v. Souza*, 223 F.3d 1197, 1201-02 (10th Cir. 2000)(Police must “instigate, orchestrate, encourage or exceed the scope of the private search to trigger the application of the Fourth Amendment”); *United States v. Reed*, 15 F.3d 928, 931 (9th Cir. 1994)(inquiry is “(1) whether the government knew of and acquiesced in the intrusive conduct; and (2) whether the party performing the search intended to assist law enforcement efforts or further his own ends”); *see also United States v. Van Dyke*, 2010 WL 1949640 at \*3 (W.D.Mich, May 14, 2010)(“permitting the government to circumvent the limits of the Fourth Amendment by directing individuals to conduct searches that the government cannot, would totally undermine the purposes of the Fourth Amendment”).

This standard is plainly met in this case, particularly with respect to the continuing packet capture of electronic communications to Swartz’s netbook and the real-time provision of DHCP log information from January 4, 2011, through January 6, 2011.<sup>10</sup> Once S/A Pickett and Det. Murphy arrived on the scene, it became a law enforcement investigation. Once the netbook was located, no further investigation was necessary to protect MIT’s rights or property. The investigation which began with the arrival of S/A Pickett and Det. Murphy was a law enforcement investigation with the object of identifying, arresting, and prosecuting the individual responsible for the downloads from

---

<sup>10</sup> *See Motion to Suppress All Fruits of Interceptions and Disclosures of Electronic Communications and Other Information by MIT Personnel in Violation of the Fourth Amendment and the Stored Communications Act and Incorporated Memorandum of Law.*

JSTOR. The netbook was left in place, with MIT continuing to monitor it at the recommendation of S/A Pickett and upon the urging of Det. Murphy. *See* page 3, *supra*. The monitoring strategy was developed in consultation with S/A Pickett and Det. Murphy. The monitoring was continued because law enforcement wanted to gather evidence of intent and motive, *see* page 6, *supra*, matters of no relevance whatsoever to the protection of MIT's interests. MIT recognized on January 4, 2011, that "[t]he investigation ha[d] moved beyond MIT was [was] now being handled by law enforcement." Exhibit 22. MIT personnel asked S/A Pickett on January 5, 2011, "what the next step [was]," Exhibit 25, further illustrating S/A Pickett's direction of the investigation. Halsall admitted that he was "gathering up all the stuff for Pickett." Exhibit 26. MIT personnel asked S/A Pickett's permission before taking the netbook offline and asked him whether they should image the netbook. *See* page 6, *supra*. In an email from Halsall to S/A Pickett on January 8, 2011, Halsall told Pickett that he "hop[ed] to have the pcap/flows/videos/logs all in by to me Monday, possibly sooner – if you don't already have a copy of the video or pcap [packet capture], I'll make sure you get one." Exhibit 2.

Here, the government plainly encouraged the search, played a role in its design and operation, and MIT personnel deferred to the guidance of law enforcement officers, aiming to assist the government in its criminal investigation rather than being motivated by its own interests. Beginning with the arrival of S/A Pickett and Det. Murphy on January 4, 2011, MIT personnel were acting as government agents, and the requirements of the Fourth Amendment are fully applicable to any search or interception of electronic communications conducted by them. These interceptions were unlawful in the absence of a warrant, issued upon a showing of probable cause. The intercepted communications, as well as all derivative fruits thereof, must be suppressed.



Respectfully submitted,  
By his attorney,

**/s/ Martin G. Weinberg**

Martin G. Weinberg  
20 Park Plaza, Suite 1000  
Boston, MA 02116  
(617) 227-3700 (tel.)  
(617) 338-9538 (fax)  
owlmgw@att.net

#### **CERTIFICATE OF SERVICE**

I, Martin G. Weinberg, hereby certify that on this 5th day of October, 2012, a copy of the foregoing document has been served via the Court's ECF system on all registered participants, including Stephen P. Heymann, AUSA. One copy of the exhibits to the motion was served on the government by hand this same date.

**/s/ Martin G. Weinberg**

Martin G. Weinberg

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

_____	)	
UNITED STATES	)	
	)	
v.	)	No. 11-10260-NMG
	)	
AARON SWARTZ	)	
_____	)	

**MOTION TO SUPPRESS ALL FRUITS OF UNLAWFUL ARRESTS WITHOUT  
PROBABLE CAUSE AND SEARCH OF HP USB DRIVE AND INCORPORATED  
MEMORANDUM OF LAW  
(MOTION TO SUPPRESS NO. 3)**

Now comes the defendant Aaron Swartz and respectfully moves that this Honorable Court suppress as evidence at the trial of this case all evidence derived from the search of his HP USB drive.

As reason therefor, defendant states:

1. He had a reasonable expectation of privacy in his USB drive.<sup>1</sup>
2. The USB drive was seized from him on January 6, 2011, during a search of his backpack incident to his arrest on state charges of breaking and entering in violation of M.G.L. c.266, §18.
3. His arrest was unlawful because not supported by probable cause to believe that he had committed the crime of breaking and entering.
3. On February 9, 2011, Secret Service S/A Michael Pickett obtained a warrant to search the USB drive; that warrant expired before it was executed, and another warrant to search the USB drive was obtained on February 24, 2011. *See* Exhibit 29. The USB drive was subsequently searched

---

<sup>1</sup> All averments herein regarding Swartz's ownership and possession of the USB drive are made pursuant to the protections provided by *Simmons v. United States*, 390 U.S. 377, 392-94 (1968).

pursuant to the warrant.

4. The affidavit in support of the search of the USB drive, *see* Exhibit 30, failed to establish probable cause to believe that it contained evidence of a crime, in violation of the Fourth Amendment.

5. All fruits of Swartz's unlawful arrest and the search of the USB drive must, accordingly, be suppressed.

**THE DEFENDANT REQUESTS A HEARING ON THE WITHIN MOTION.**

**LOCAL RULE 7.1(A)(2) STATEMENT**

The undersigned counsel has conferred with AUSA Stephen Heymann. The government opposes the suppression remedies sought and will respond to defendant's request for a hearing in its response to the motion.

**MEMORANDUM OF LAW**

**I. BACKGROUND.**

On January 6, 2011, Swartz was arrested on state charges of breaking and entering in violation of M.G.L. c.266, §18. *See* Exhibit 31 at 2. The backpack Swartz was carrying was searched and his USB drive, which was in his backpack, was seized. Secret Service S/A Michael Pickett subsequently applied for, and obtained a warrant to search the USB drive. The sum total of the information regarding the USB drive contained in the affidavit submitted in support of the application for a warrant to search the USB drive was:

25. An MIT police officer who had seen several pictures taken by the covert camera in Building 16's network wiring closet saw Aaron Swartz on a bicycle near MIT, approximately half an hour after the "ghost laptop" had been connected in Building W20. The officer stopped his car, activated its blue lights and displayed his wallet badge. When he sought to question Swartz, Swartz dropped his bike to the ground and fled. The backpack

in Swartz's possession at the time he was caught and arrested minutes later appeared to be the same one he had with him on each occasion he was videotaped in the wiring closet at MIT.

26. In the backpack was the USB DRIVE. From my training and experience and information provided to me by other agents, USB drives are frequently used to store software applications, data and records, including .pdf formatted records such as those that were illegally downloaded from JSTOR. They are also frequently used to transfer records and data between computers or hard drives, such as those connected in the wiring closet to MIT's network and ones available to Swartz outside.

Exhibit 30 at 7.<sup>2</sup>

## **II. SWARTZ'S ARREST WAS UNLAWFUL BECAUSE NOT SUPPORTED BY PROBABLE CAUSE TO BELIEVE THAT HE COMMITTED THE MASSACHUSETTS OFFENSE OF BREAKING AND ENTERING.**

It is axiomatic that, for an arrest to be lawful, it must be predicated on probable cause. *See Glik v. Cunniffe*, 655 F.3d 78, 85 (1st Cir. 2011) ("The Fourth Amendment requires that an arrest be grounded in probable cause"). "Probable cause exists when police officers, relying on reasonably trustworthy facts and circumstances, have information upon which a reasonably prudent person would believe the suspect had committed or was committing a crime." *United States v. Pontoo*, 666 F.3d 20, 31 (1st Cir. 2011), *quoting United States v. Young*, 105 F.3d 1, 6 (1st Cir. 1997). That standard was not satisfied in this case.

Swartz was arrested on charges of breaking and entering in violation of M.G.L. c.266, §18, which provides:

Whoever, in the night time, enters a dwelling house without breaking, or breaks and enters in the day time a building, ship or motor vehicle or vessel, with intent to commit a felony, no person lawfully therein being put in fear, shall be punished by imprisonment in the state

---

<sup>2</sup> Other than the fact that the USB drive was in the backpack, the information set forth in paragraph 26 was not included in the original February 9, 2011, affidavit, *i.e.*, the affidavit said nothing regarding what a USB drive is and what it might be used for. That affidavit also erroneously stated that Swartz "dropped his bike *and backpack* to the ground and fled," Exhibit 32 at 7 (emphasis added), as S/A Pickett admits at page 7 n.5 of his February 24, 2011, affidavit.

prison for not more than ten years or by a fine of not more than five hundred dollars and imprisonment in jail for not more than two years. . . .

The first requirement under §18 is that there must have been a “breaking.” While the opening of a closed but unlocked door is a breaking, passing through an unobstructed entrance is not. *Commonwealth v. Lewis*, 346 Mass. 373, 377 (1963). Thus, to have probable cause to arrest Swartz, the arresting officers must have had probable cause to believe that he in fact opened a door to enter the data room in which the laptop was discovered. Moreover, MIT is an open campus, and the data room was located on a corridor along which classrooms were located and along which people frequently passed to access classrooms or to travel between MIT buildings. There was no notice on the exterior of the data room indicating that access was prohibited. *See* Exhibit 27. Inherent in the offense of breaking and entering is the requirement that the defendant break and enter into premises where he has no permission to be, a proposition that Massachusetts case law clearly supports. *See, e.g., Commonwealth v. LeClaire*, 28 Mass. App. Ct. 932, 933 (1990)(upholding breaking and entering conviction where defendant broke into room *where he had no permission or authority to be*). There was nothing here which gave Swartz any reason to believe that he could not permissibly enter the room.

Second, “[i]n the lexicon of Massachusetts crimes there is no such crime as ‘breaking and entering’ unaccompanied by intent to commit a felony or misdemeanor.” *Commonwealth v. Vinnicombe*, 28 Mass. App. Ct. 934, 934 (1990). *See, e.g., Commonwealth v. Walter*, 40 Mass. App. Ct. 907, 909 (1996)(“The ‘intent to commit a felony’ is an essential element of the crime proscribed by G.L. c.266, §18, breaking and entering in the daytime with intent to commit a felony”). Accordingly, there could have been no probable cause to arrest Swartz unless the arresting officers

had probable cause to believe that his intent in entering the data room was to commit a felony. The Cambridge Police Department Incident Report of the arrest does not specify the felony at issue, but, as Swartz was charged in state court with breaking and entering with the intent to commit larceny on January 4 and 6, 2011, Swartz will proceed herein on the assumption that that was the offense which the arresting officers believed provided a valid basis for his arrest. It did not. The Massachusetts larceny statute, M.G.L. c.266, §30, provides in pertinent part:

(1) Whoever steals, or with intent to defraud obtains by a false pretence, or whoever unlawfully, and with intent to steal or embezzle, converts, or secretes with intent to convert, the property of another as defined in this section, whether such property is or is not in his possession at the time of such conversion or secreting, shall be guilty of larceny, and shall . . . if the value of the property stolen exceeds two hundred and fifty dollars, be punished by imprisonment in the state prison for not more than five years, or by a fine of not more than twenty-five thousand dollars and imprisonment in jail for not more than two years; or, if the value of the property stolen . . . does not exceed two hundred and fifty dollars, shall be punished by imprisonment in jail for not more than one year or by a fine of not more than three hundred dollars . . . .

(2) The term “property”, as used in the section, shall include money, personal chattels, a bank note, bond, promissory note, bill of exchange or other bill, order or certificate, a book of accounts for or concerning money or goods due or to become due or to be delivered, a deed or writing containing a conveyance of land, any valuable contract in force, a receipt, release or defeasance, a writ, process, certificate of title or duplicate certificate issued under chapter one hundred and eighty-five, a public record, anything which is of the realty or is annexed thereto, a security deposit received pursuant to section fifteen B of chapter one hundred and eighty-six, electronically processed or stored data, either tangible or intangible, data while in transit, telecommunications services, and any domesticated animal, including dogs, or a beast or bird which is ordinarily kept in confinement.

Thus, to have had probable cause to believe that Swartz entered the data room with the intent to commit larceny, the arresting officers must have had probable cause to believe that he either intended to steal property or to obtain property by false pretenses with the intent to defraud.<sup>3</sup> An essential

---

<sup>3</sup> The third alternative, embezzlement, is inapplicable here because embezzlement requires that the defendant “fraudulently converted to his personal use property that was under his control by

element of the “stealing” form of larceny is the “intent to deprive the person of the property permanently.” *Commonwealth v. Christian*, 430 Mass. 552, 558 (2000). *See, e.g., Commonwealth v. Sullivan*, 40 Mass. App. Ct. 284, 287 (1996)(“Larceny consists of (1) the taking or carrying away of property (2) that belongs to another person (3) with the intent to deprive that person of the property permanently”). Nothing which Swartz did in downloading journal articles from JSTOR was intended to deprive JSTOR of its property permanently, nor did the downloading even have that effect. JSTOR remained at all times in full possession of its property, and nothing Swartz did on January 4-6, 2011, prevented others from gaining access to, and using, the JSTOR archives. There is nothing in Massachusetts law which recognizes the electronic copying of data as larceny.<sup>4</sup> Accordingly, there was no probable cause to arrest Swartz for breaking and entering to commit larceny by stealing.

Nor was there probable cause to arrest Swartz for larceny by false pretenses. The crime of

---

virtue of a position of ‘trust or confidence’ and did so with the intent to deprive the owner of the property permanently.” *Commonwealth v. Mills*, 436 Mass. 387, 394 (2002).

<sup>4</sup> That copying of electronically-available data is not encompassed within §30(1) is underscored by the provisions of §30(4):

Whoever steals, or with intent to defraud obtains by a false pretense, or whoever unlawfully, and with intent to steal or embezzle, converts, secretes, unlawfully takes, carries away, conceals *or copies* with intent to convert any trade secret of another, regardless of value, whether such trade secret is or is not in his possession at the time of such conversion or secreting, shall be guilty of larceny . . . .

(emphasis added). The inclusion of copying in subsection (4) but not in subsection (1) evidences an intent that copying does not violate subsection (1), as it does not permanently deprive the owner of its property. Copying violates the statute only in cases of trade secrets, which are not at issue here. *See* §30(4)(defining “trade secrets” as “anything tangible or intangible or electronically kept or stored, which constitutes, represents, evidences or records a secret scientific, technical, merchandising, production or management information, design, process, procedure, formula, invention or improvement”).

larceny by false pretenses “requires proof that (1) a false statement of fact was made; (2) the defendant knew or believed that the statement was false when he made it; (3) the defendant intended that the person to whom he made the false statement would rely on it; and (4) the person to whom the false statement was made did rely on it and, consequently, parted with property.” *Commonwealth v. McCauliff*, 461 Mass. 635, 639-39 (2012). *See, e.g., Commonwealth v. Mills*, 436 Mass. 387, 396-97 (2002); *Commonwealth v. Gall*, 58 Mass. App. Ct. 278, 285 (2003). First, Swartz made no false statements of fact on January 4-6, 2011. Second, even if he had made a false statement, it was not made to *JSTOR*, nor was it made with the intent that *JSTOR* would rely on it, *JSTOR* did not rely on any false statement by Swartz, and no false statements by Swartz caused *JSTOR* to part with its property. Third, *JSTOR* did not “part with” its property. It simply permitted Swartz to access it and download it; *JSTOR* continued to maintain full possession of its property. There was, accordingly, no probable cause to arrest Swartz for breaking and entering to commit larceny by false pretenses. Because Swartz’s arrest was unlawful, all fruits of that unlawful arrest, including, but not limited to, his USB drive, must be suppressed.

**III. EVEN SHOULD THIS COURT CONCLUDE THAT SWARTZ’S ARREST WAS LAWFUL, THE FRUITS OF THE SEARCH OF THE USB DRIVE MUST NONETHELESS BE SUPPRESSED BECAUSE THE AFFIDAVIT FAILED TO ESTABLISH PROBABLE CAUSE FOR THE SEARCH OF THE USB DRIVE.**

Probable cause exists when “the affidavit upon which a warrant is founded demonstrates in some trustworthy fashion the likelihood that an offense has been committed and that there is sound reason to believe that a particular search will turn up evidence of it.” *United States v. Schaefer*, 87 F.3d 562, 565 (1st Cir. 1996), *quoting United States v. Aguirre*, 839 F.2d 854, 857-58 (1st Cir. 1988). “[M]ere suspicion, rumor, or strong reason to suspect [wrongdoing]’ are not sufficient.”



*United States v. Vigeant*, 176 F.3d 565, 569 (1st Cir. 1999). Instead, the affidavit must provide the issuing judge with a “substantial basis” for concluding that probable cause exists. *See, e.g., United States v. Feliz*, 182 F.3d 82, 86 (1st Cir. 1999); *United States v. Khounsavanh*, 113 F.3d 279, 283 (1st Cir.1997).

While courts often speak of the need to accord deference to the issuing judge’s “assessment of the facts and inferences supporting the affidavit,” *United States v. Sawyer*, 144 F.3d 191, 193 (1st Cir. 1998), “[d]eference to the [issuing] magistrate . . . is not boundless.” *United States v. Leon*, 468 U.S. 897, 914 (1984). *See, e.g., United States v. Danhauer*, 229 F.3d 1002, 1006 (10th Cir. 2000)(court will not defer to magistrate if there is not substantial basis for concluding that probable cause existed). Such deference does not, for example, extend to permit the upholding of a warrant based on conclusory allegations by the affiant. *See, e.g., Vigeant*, 176 F.3d at 571; *United States v. Wilhelm*, 80 F.3d 116, 119 (4th Cir.1996). “Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others.” *Illinois v. Gates*, 462 U.S. 213, 239 (1983). *See also Johnson v. United States*, 333 U.S. 10, 14 (1947); *Khounsavanh*, 113 F.3d at 284. Probable cause is a fact-specific inquiry, and it is, in each case, “the duty of a court confronted with the question to determine whether the facts and circumstances of the particular [affidavit in support of a warrant application] justified the issuance of the warrant.” *Id.* at 285. *See also United States v. Weaver*, 99 F.3d 1372, 1376-77 (6th Cir.1996).

“A warrant application must demonstrate probable cause to believe that (1) a crime has been committed – the ‘commission’ element, and (2) enumerated evidence of the offense will be found at the place to be searched – the . . . ‘nexus’ element.” *United States v. Ribeiro*, 397 F.3d 43, 48 (1st

Cir. 2005), *quoting Feliz*, 182 F.3d at 86. S/A Pickett’s affidavit is fatally deficient as to the second requirement – it fails to establish probable cause to believe that evidence of the alleged crime would be found on the USB drive. Whether there is probable cause to believe that the suspect has committed a crime and whether there is a nexus between evidence of that crime and the place or item to be searched are two separate inquiries; probable cause to believe that someone has committed a crime does not *ipso facto* provide probable cause to believe that evidence of that crime will be found within a closed container belonging to him. “The critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific ‘things’ to be searched for and seized are located on the property to which entry is sought.” *Zurcher v. Stanford Daily*, 436 U.S. 547, 556 (1978). There must be “some type of evidence connecting the criminal activity, not just the suspect, to the place to be searched.” *United States v. Kemper*, 375 F.Supp.2d 551, 553 (E.D.Ky. 2005). *See, e.g., United States v. Rosario*, 918 F.Supp. 524, 531 (D.R.I. 1996); *United States v. Rios*, 881 F.Supp. 772, 775 (D.Conn. 1995); *United States v. Stout*, 641 F.Supp. 1074, 1078 (N.D.Cal. 1986). Any contrary rule “would be an open invitation to vague warrants authorizing virtually automatic searches of any property used by a criminal suspect.” *Rosario*, 918 F.Supp. at 531. *See also United States v. Schultz*, 14 F.3d 1093, 1098 (6th Cir. 1994); *Rios*, 881 F.Supp. at 775; *Stout*, 641 F.Supp. at 1078.

Here, the requisite nexus is absent. Swartz may have been carrying the USB drive in his backpack, and that backpack may have accompanied him when he visited the basement data room at MIT, but what is entirely missing is any connection between the USB drive and the alleged offense. The possession of a USB drive connotes nothing nefarious. Quite the contrary, USB drives – often referred to as thumb drives or flash drives or memory sticks – are common accoutrements

of modern life, used by millions of people every day for storing and transporting a wide variety of personal and professional documents, as well as other information, and, for example, photographs, videos, audio files, and games. *See* [http://en.wikipedia.org/wiki/USB\\_flash\\_drive](http://en.wikipedia.org/wiki/USB_flash_drive). The videotape never showed Swartz using the USB drive in connection with the JSTOR downloads. Quite the contrary, in fact. The videotape showed a far larger external hard drive attached to the ACER laptop which was connected to the MIT network and showed Swartz retrieving one hard drive and exchanging it for another, *i.e.*, it showed that, to the extent that Swartz was using any portable medium to store and transport downloaded JSTOR data, it was not a USB drive but instead an external hard drive. Neither the laptop nor the hard drive was in Swartz's backpack when it was seized but were instead seized later from a separate location at MIT.

While S/A Pickett did add some experiential generalities about what USB drives can be used for, there is nothing in the affidavit which factually connects those potential uses to the circumstances of this particular case. Such generalities are entitled to little or no weight, as the affidavit did not provide a sufficient factual basis for the Magistrate Judge to make a neutral, independent determination that the generalities recited by S/A Pickett were likely to be true with respect to the particular search for which authorization was being sought. *See, e.g., Ribeiro*, 397 F.3d at 52 (generalizations alone may not be enough to satisfy the nexus element); *Zimmerman*, 277 F.3d 416, 433 n.3 (3d Cir. 2002) (expert opinion "must be tailored to the specific facts of the case to have any value"); *Schultz*, 14 F.3d at 1097 (officer's training and experience "cannot substitute for the lack of evidentiary nexus"). The affidavit failed to establish probable cause for the search of the USB drive.

**IV. THE GOOD FAITH EXCEPTION CANNOT SAVE THE SEARCH OF THE USB DRIVE, AND ALL FRUITS OF THAT SEARCH MUST BE SUPPRESSED.**

The government has the burden to demonstrate the applicability of the good faith exception, *see, e.g., United States v. Diehl*, 276 F.3d 32, 42 (1st Cir. 2002), and unless it can meet that burden, the evidence must be suppressed. It will not be able to do so in this case. “Although weakening the exclusionary rule, the [*Leon*] Court did not defenestrate it.” *United States v. Ricciardelli*, 998 F.2d 8, 15 (1st Cir. 1993). “Good faith is not a magic lamp for police officers to rub whenever they find themselves in trouble.” *United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir. 1996), *aff’d on rehearing*, 91 F.3d 331 (1996). The determination whether the *Leon* good faith exception should be applied in a particular case requires an “inquir[y] into the ‘objectively ascertainable question whether a reasonably well-trained officer would have known that the search was illegal despite the magistrate’s authorization.’” *United States v. Diaz*, 841 F.2d 1, 5 (1st Cir. 1998), *quoting United States v. Leon*, 468 U.S. 897, 922 n.23 (1984).

The good faith exception does not apply when the affidavit was “so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.” *Leon*, 468 U.S. at 922. Where the defect in the warrant is one of probable cause, the requisite inquiry is “whether a reasonably well-trained officer . . . would have known that his affidavit failed to establish probable cause and that he should not have applied for the warrant.” *Vigeant*, 176 F.3d at 571, *quoting Malley v. Briggs*, 475 U.S. 335, 345 (1985). Here, a reasonably well-trained officer would have known that the affidavit failed to establish probable cause as to the essential “nexus” element of probable cause. *See, e.g., United States v. Grant*, 682 F.3d 827, 841 (9th Cir. 2012); *United States v. Laughton*, 409 F.3d 744, 749 (6th Cir. 2005); *Zimmerman*, 277 F.3d at 437-38; *Kemper*, 375 F.Supp.2d at 554-55.

The Court should, therefore, find the good faith exception inapplicable.

### **CONCLUSION**

For all the foregoing reasons, all fruits of Swartz's unlawful arrest and the search of the USB drive must be suppressed as evidence at the trial of this case.

Respectfully submitted,  
By his attorney,

**/s/ Martin G. Weinberg**

Martin G. Weinberg  
20 Park Plaza, Suite 1000  
Boston, MA 02116  
(617) 227-3700 (tel.)  
(617) 338-9538 (fax)  
owlmgw@att.net

### **CERTIFICATE OF SERVICE**

I, Martin G. Weinberg, hereby certify that on this 5th day of October, 2012, a copy of the foregoing document has been served via the Court's ECF system on all registered participants, including Stephen P. Heymann, AUSA. One copy of the exhibits to the motion was served on the government by hand this same date.

**/s/ Martin G. Weinberg**

Martin G. Weinberg

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES	)	
	)	
v.	)	No. 11-10260-NMG
	)	
AARON SWARTZ	)	
	)	

**MOTION TO SUPPRESS ALL FRUITS OF SEARCHES PURSUANT TO A WARRANT  
OF 950 MASSACHUSETTS AVENUE, APT. 320, CAMBRIDGE, MASSACHUSETTS,  
AND 124 MOUNT AUBURN STREET, OFFICE 504, CAMBRIDGE, MASSACHUSETTS  
AND INCORPORATED MEMORANDUM OF LAW  
(MOTION TO SUPPRESS NO. 4)**

Now comes the defendant Aaron Swartz and respectfully moves that this Honorable Court suppress as evidence at the trial of this case all evidence derived from searches of his home at 950 Massachusetts Avenue, Apt. 320, Cambridge, Massachusetts, and of his office at 124 Mount Auburn Street, Office 504, Cambridge, Massachusetts.

As reason therefor, defendant states:

1. He had a reasonable expectation of privacy in his home and in his office.
2. On February 9, 2011, Secret Service S/A Michael Pickett submitted an affidavit in support of an application for a warrant to search Swartz's home at 950 Massachusetts Avenue, Apt. 320, Cambridge, Massachusetts. Exhibit 34. A warrant authorizing the search was issued the same day. Exhibit 35. The search warrant was executed on February 11, 2011.
3. The affidavit submitted in support of the warrant application failed to establish probable cause to believe that evidence of the alleged offense would be found in Swartz's home, in violation of the Fourth Amendment.
4. On February 11, 2011, Secret Service S/A Brett Seidel submitted an affidavit in support

of an application for a warrant to search Swartz's office at 124 Mount Auburn Street, Office 504, Cambridge, Massachusetts, the case-specific averments of which were virtually entirely derived from observations made by law enforcement officers during the search of Swartz's home and statements made by Swartz which were a direct product of that search. Exhibit 36. The warrant was issued and executed the same day. Exhibit 37.

5. The warrant to search Swartz's office was devoid of probable cause to believe that the items sought would be located there. The probable cause averments of the affidavit were derived from the unlawful search of his home; with those portions of the affidavit excised, as they must be, the affidavit failed to establish probable cause for the search. Alternatively, even if the earlier search of his home were found not to have violated the Fourth Amendment, the affidavit did not establish probable cause to search Swartz's office.

6. All fruits of both searches must, accordingly, be suppressed.

**THE DEFENDANT REQUESTS A HEARING ON THE WITHIN MOTION.**

**LOCAL RULE 7.1(A)(2) STATEMENT**

The undersigned counsel has conferred with AUSA Stephen Heymann. The government opposes the suppression remedies sought and will respond to defendant's request for a hearing in its response to the motion.

**MEMORANDUM OF LAW**

**I. THE SEARCH OF SWARTZ'S HOME.**

**A. Swartz Had A Reasonable Expectation of Privacy in his Home.**

"An individual's right to be free from unreasonable searches is implicated when he or she (1) has "manifested a subjective expectation of privacy" in the place searched, which (2) "society

accepts as objectively reasonable.” *United States v. Cardona-Sandoval*, 6 F.3d 15, 20 (1st Cir. 1993), *quoting California v. Greenwood*, 486 U.S. 35, 39 (1988). *See, e.g., United States v. Mancini*, 8 F.3d 104, 107 (1st Cir. 1993). The apartment at 950 Massachusetts Avenue, Apt. 320, Cambridge, Massachusetts, was Swartz’s home at the time of the search. He had a subjective expectation of privacy in his home, and that expectation is one which society would certainly accept as objectively reasonable.

**B. The Averments of the Affidavit.**

After reciting information based on which S/A Pickett believed that a crime had been committed and that Swartz had committed it, none of which was in any way related to Swartz’s home, Exhibit 34 at 3-7, the affidavit had only this to say about Swartz’s home:

26. It is probable that Aaron Swartz stores and uses computer equipment, computer hardware, computer software, computer related documentation, data and records, as defined in Attachment B, at 950 Massachusetts Avenue, Apartment 320, Cambridge, Massachusetts, where he lives.

\* \* \* \* \*

30. Swartz has provided 950 Massachusetts Avenue, Apartment 320, Cambridge, Massachusetts to the Commonwealth as his home address. It is also the address of record for Demand Progress, Inc., of which he is the registered agent, director, president and treasurer. Demand Progress maintains a website, in which it describes its mission in part to seek progressive policy changes by running online campaigns.

Exhibit 34 at 7 -8.<sup>1</sup> The affidavit also mentioned that neither the “ghost macbook” associated with the JSTOR downloading or the external hard drive which had been observed attached to the ACER laptop on January 4, 2011, had yet been recovered. *Id.* The affidavit further stated that on January 10, 2011, Swartz “broadcast a message via Twitter for Mac.” *Id.* Finally, S/A Pickett included a boilerplate recitation of the purposes for which individuals in general use computers, noting that 86%

---

<sup>1</sup> Paragraph 31 of the affidavit goes on to provide a description of the premises.



of all households owned at least one computer. *Id.* at 8.

**C. The Affidavit Failed to Establish Probable Cause to Believe That the Items Sought Would Be Located At Swartz's Home at the Time of the Search.**

Probable cause exists when “the affidavit upon which a warrant is founded demonstrates in some trustworthy fashion the likelihood that an offense has been committed and that there is sound reason to believe that a particular search will turn up evidence of it.” *United States v. Schaefer*, 87 F.3d 562, 565 (1st Cir. 1996), *quoting United States v. Aguirre*, 839 F.2d 854, 857-58 (1st Cir. 1988). “[M]ere suspicion, rumor, or strong reason to suspect [wrongdoing]’ are not sufficient.” *United States v. Vigeant*, 176 F.3d 565, 569 (1st Cir. 1999). Instead, the affidavit must provide the issuing judge with a “substantial basis” for concluding that probable cause exists. *See, e.g., United States v. Feliz*, 182 F.3d 82, 86 (1st Cir. 1999); *United States v. Khounsavanh*, 113 F.3d 279, 283 (1st Cir.1997).

While courts often speak of the need to accord deference to the issuing judge’s “assessment of the facts and inferences supporting the affidavit,” *United States v. Sawyer*, 144 F.3d 191, 193 (1st Cir. 1998), “[d]eference to the [issuing] magistrate . . . is not boundless.” *United States v. Leon*, 468 U.S. 897, 914 (1984). *See, e.g., United States v. Danhauer*, 229 F.3d 1002, 1006 (10th Cir. 2000)(court will not defer to magistrate if there is not substantial basis for concluding that probable cause existed). Such deference does not, for example, extend to permit the upholding of a warrant based on conclusory allegations by the affiant. *See, e.g., Vigeant*, 176 F.3d at 571; *United States v. Wilhelm*, 80 F.3d 116, 119 (4th Cir.1996). “Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others.” *Illinois v. Gates*, 462 U.S. 213, 239 (1983). *See also Johnson*

*v. United States*, 333 U.S. 10, 14 (1947); *Khounsavanh*, 113 F.3d at 284. Probable cause is a fact-specific inquiry, and it is, in each case, “the duty of a court confronted with the question to determine whether the facts and circumstances of the particular [affidavit in support of a warrant application] justified the issuance of the warrant.” *Id.* at 285. *See also United States v. Weaver*, 99 F.3d 1372, 1376-77 (6th Cir.1996).

“A warrant application must demonstrate probable cause to believe that (1) a crime has been committed – the ‘commission’ element, and (2) enumerated evidence of the offense will be found at the place to be searched – the . . . ‘nexus’ element.” *United States v. Ribeiro*, 397 F.3d 43, 48 (1st Cir. 2005), *quoting United States v. Feliz*, 182 F.3d 82, 86 (1st Cir. 1999). In deciding whether the affidavit demonstrates such the requisite nexus between the items sought and the place to be searched, the judicial officer must determine “whether the totality of circumstances reasonably inferable from the affidavit demonstrates a ‘fair probability’ that evidence material to the ‘commission’ of the probable crime will be disclosed at the search premises at about the time the search warrant would issue . . . .” *United States v. Zayas-Diaz*, 95 F.3d 105, 113 (1st Cir. 1996). *See, e.g., Ribeiro*, 397 F.3d at 48-49; *Feliz*, 182 F.3d at 86. Nexus need not rest on any direct observation, but may be inferred from the type of crime, the nature of the items sought, the extent of an opportunity for concealment and normal inferences as to where a criminal would hide [evidence of the crime].” *Feliz*, 182 F.3d at 88.

Whether there is probable cause to believe that the suspect has committed a crime and whether there is a nexus between evidence of that crime and the place to be searched are two separate inquiries; probable cause to believe that someone has committed a crime does not *ipso facto* provide probable cause to believe that evidence of that crime will be found in his home or office.

“The critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific ‘things’ to be searched for and seized are located on the property to which entry is sought.” *Zurcher v. Stanford Daily*, 436 U.S. 547, 556 (1978). There must be “some type of evidence connecting the criminal activity, not just the suspect, to the place to be searched.” *United States v. Kemper*, 375 F.Supp.2d 551, 553 (E.D.Ky. 2005). *See, e.g., United States v. Rosario*, 918 F.Supp. 524, 531 (D.R.I. 1996); *United States v. Rios*, 881 F.Supp. 772, 775 (D.Conn. 1995); *United States v. Stout*, 641 F.Supp. 1074, 1078 (N.D.Cal. 1986). Any contrary rule “would be an open invitation to vague warrants authorizing virtually automatic searches of any property used by a criminal suspect.” *Rosario*, 918 F.Supp. at 531. *See also United States v. Schultz*, 14 F.3d 1093, 1098 (6th Cir. 1994); *Rios*, 881 F.Supp. at 775; *Stout*, 641 F.Supp. at 1078.

S/A Pickett’s affidavit completely failed to demonstrate probable cause to believe that the items sought would be found in Swartz’s home at the time of the search. The warrant was applied for, and issued, more than a month after Swartz was arrested on January 6, 2011. The alleged offenses at issue were not shown to have had any connection to Swartz’s home. The laptops through which the JSTOR downloads were conducted were located on MIT premises and used the MIT network to access JSTOR. Swartz was not observed going from his apartment to MIT or going directly from accessing the laptop and hard drive at MIT to his apartment. Nothing in the affidavit even inferentially connects the items sought with Swartz’s apartment. *Compare, e.g., United States v. Laughton*, 409 F.3d 744, 474 (6th Cir. 2005)(ordering evidence suppressed where affidavit failed to make any connection between the residence to be searched and the facts of the criminal activity set forth in the affidavit); *Kemper*, 375 F.Supp.2d at 554 (ordering evidence suppressed where no

nexus shown between residence and the criminal activity as to which evidence sought), *with, e.g., Ribeiro*, 397 F.3d at 52 (affidavit set forth police observations of defendant leaving residence in close temporal proximity to drug transactions); *United States v. Keene*, 341 F.3d 78, 82 (1st Cir. 2003)(fact that defendant worked from home while recovering from injury suggested that drug distribution was being organized from defendant's home). Even if one indulged in the unwarranted assumption that the twitter message referenced by S/A Pickett was sent from the same macbook used during the JSTOR downloads, the macbook, being readily portable, could have been located anywhere when the message was sent; this information provides no nexus between the macbook and Swartz's apartment. On the critical nexus component of the probable cause calculus, the affidavit provided the Magistrate Judge with little more than S/A Pickett's bare-bones claim that "[i]t is probable" that the items sought would be found at Swartz's home.<sup>2</sup> Such conclusory allegations by the affiant, not even accompanied by standard boilerplate regarding what the affiant's training and experience tell him about where individuals maintain evidence of crimes, does not suffice to establish probable cause.

**D. The Good Faith Exception Cannot Save the Search of Swartz's Home, and All Fruits of That Search must Be Suppressed.**

The government has the burden to demonstrate the applicability of the good faith exception,

---

<sup>2</sup> While S/A Pickett did add some experiential generalities about what computers can be used for, there is nothing in the affidavit which factually connects those potential uses to the circumstances of this particular case. Such generalities are entitled to little or no weight, as the affidavit did not provide a sufficient factual basis for the Magistrate Judge to make a neutral, independent determination that the generalities recited by S/A Pickett were likely to be true with respect to the particular search for which authorization was being sought. *See, e.g., Ribeiro*, 397 F.3d at 52 (generalizations alone may not be enough to satisfy the nexus element); *Zimmerman*, 277 F.3d 416, 433 n.3 (3d Cir. 2002)(expert opinion "must be tailored to the specific facts of the case to have any value"); *Schultz*, 14 F.3d at 1097 (officer's training and experience "cannot substitute for the lack of evidentiary nexus").

*see, e.g., United States v. Diehl*, 276 F.3d 32, 42 (1st Cir. 2002), and unless it can meet that burden, the evidence must be suppressed. It will not be able to do so in this case. “Although weakening the exclusionary rule, the [*Leon*] Court did not defenestrate it.” *United States v. Ricciardelli*, 998 F.2d 8, 15 (1st Cir. 1993). “Good faith is not a magic lamp for police officers to rub whenever they find themselves in trouble.” *United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir. 1996), *aff’d on rehearing*, 91 F.3d 331 (1996). The determination whether the *Leon* good faith exception should be applied in a particular case requires an “inquir[y] into the ‘objectively ascertainable question whether a reasonably well-trained officer would have known that the search was illegal despite the magistrate’s authorization.’” *United States v. Diaz*, 841 F.2d 1, 5 (1st Cir. 1998), *quoting United States v. Leon*, 468 U.S. 897, 922 n.23 (1984).

The good faith exception does not apply when the affidavit was “so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.” *Leon*, 468 U.S. at 922. Where the defect in the warrant is one of probable cause, the requisite inquiry is “whether a reasonably well-trained officer . . . would have known that his affidavit failed to establish probable cause and that he should not have applied for the warrant.” *Vigeant*, 176 F.3d at 571, *quoting Malley v. Briggs*, 475 U.S. 335, 345 (1985). Here, a reasonably well-trained officer would have known that the affidavit failed to establish probable cause as to the essential “nexus” element of probable cause. *See, e.g., United States v. Grant*, 682 F.3d 827, 841 (9th Cir. 2012); *United States v. Loughton*, 409 F.3d 744, 749 (6th Cir. 2005); *Zimmerman*, 277 F.3d at 437-38; *Kemper*, 375 F.Supp.2d at 554-55. The Court should, therefore, find the good faith exception inapplicable. Accordingly, all fruits of the search of Swartz’s home, including, but not limited to, statements made by him to law enforcement officers during the search.

## II. THE SEARCH OF SWARTZ’S OFFICE.

### A. Swartz Had a Reasonable Expectation of Privacy in his Office.

The office which was searched was Swartz’s private office at the Safra Center for Ethics at Harvard, where he was a fellow. He did not share it with others, and the door had a lock on it. The computer in the office was password-protected. He had a both a subjective and an objectively reasonable expectation of privacy in his office. *See, e.g., United States v. Ziegler*, 474 F.3d 1184, 1189-90 (9th Cir. 2007); *O’Rourke v. Hayes*, 378 F.3d 1201, 1208 (11th Cir. 2004); *United States v. Mancini*, 8 F.3d 104, 109-10 (1st Cir. 1993).

### B. The Search of Swartz’s Office Was the Derivative Fruit of the Unlawful Search of Swartz’s Home.

The probable cause averments of the affidavit are virtually entirely derived from observations made by law enforcement officers at the time of the search of Swartz’s home and statements made by Swartz during, and as the direct product of, the search – that during the search, law enforcement officers observed computer wiring and computer paraphernalia, but no computers, that Swartz said during the search, “what took you so long” and “Why didn’t you do this earlier?”, that Swartz left the building when the agents did and began running, and that Swartz was thereafter located at his office at 124 Mount Auburn Street, Suite 520N. Exhibit 36, ¶¶6-9.<sup>3</sup> Indeed, the affidavit’s nexus recitations rely virtually exclusively on the fruits of the unlawful search of Swartz’s home: “Based on Swartz’s statements during the search, the fact that computer hardware had clearly been removed from his apartment, his conduct immediately after the search, the remote access capabilities of the

---

<sup>3</sup> In ¶11, the affidavit discusses the results of the port scan of Swartz’s laptop, which was itself an unlawful search. *See* Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law.

Acer laptop installed at MIT in furtherance of the crimes, and on my training and experience, I believe that it is probable that Swartz ran from the apartment after the search to locate, hide and/or destroy evidence, fruits, or instrumentalities at his office.” Exhibit 36, ¶14. Absent the information gleaned as the direct result of the unlawful search of Swartz’s home, the affidavit does not establish probable cause to believe that evidence of the alleged offense would be found in Swartz’s office. All evidence seized pursuant to this warrant, as well as all derivative fruits thereof, must be suppressed.

**C. Even if the Information Which Was the Product of the Search of Swartz’s Home is Considered, the Affidavit Failed to Establish Probable Cause to Search Swartz’s Office.**

The information set forth in the affidavit fails to provide probable cause to believe that evidence of the alleged offenses would be found in Swartz’s office. *See* pages 4-6, *supra*. Swartz’s statements to law enforcement officers during the search of his home, on which the affiant relies, Exhibit 36, ¶¶6, 14, provide no basis for an inference that evidence of the alleged crime was located at Swartz’s office, nor do the remote capabilities of the Acer laptop, Exhibit 36, ¶¶11, 14, which had long since been seized by law enforcement. That Swartz had “computer hardware” in his office, Exhibit 36, ¶13, does not establish a connection with the alleged offenses. It is a rare office indeed in these days that does not contain computer hardware. The only computer hardware associated with the alleged offenses was the Acer laptop and the hard drive seized on January 4, 2011, and a macbook and a Samsung hard drive, and the affidavit provides no reason to believe that either of the latter two would be found in Swartz’s office. The only connection shown with Swartz’s office is that he was observed to run there after his home was searched. That observation does not provide probable cause to believe that evidence of the alleged offenses would be found in Swartz’s office; indeed, that Swartz went to his office immediately following the search of his home, going past the

officers who searched his home to do so and with them observing him, would suggest quite the opposite of his going to his office for the purpose of destroying or removing evidence.

**D. The Good Faith Exception Cannot Save the Search of Swartz's Office, and All Fruits of That Search must Be Suppressed.**

The good faith exception cannot save the unlawful search of Swartz's office for the same reasons addressed in Section I(D), *supra*.

Respectfully submitted,  
By his attorney,

**/s/ Martin G. Weinberg**  
Martin G. Weinberg  
20 Park Plaza, Suite 1000  
Boston, MA 02116  
(617) 227-3700 (tel.)  
(617) 338-9538 (fax)  
owlmgw@att.net

**CERTIFICATE OF SERVICE**

I, Martin G. Weinberg, hereby certify that on this 5th day of October, 2012, a copy of the foregoing document has been served via the Court's ECF system on all registered participants, including Stephen P. Heymann, AUSA. One copy of the exhibits to this motion was served on the government by hand this same date.

**/s/ Martin G. Weinberg**

Martin G. Weinberg



UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

_____	)	
UNITED STATES	)	
	)	
v.	)	No. 11-10260-NMG
	)	
AARON SWARTZ	)	
_____	)	

**MOTION TO SUPPRESS ALL FRUITS OF SEARCHES OF ACER LAPTOP, HP USB  
DRIVE, AND WESTERN DIGITAL HARD DRIVE AND INCORPORATED  
MEMORANDUM OF LAW  
(MOTION TO SUPPRESS NO. 5)**

Now comes the defendant Aaron Swartz and respectfully moves that this Honorable Court suppress as evidence at the trial of this case all evidence derived from the searches of his ACER laptop, his Western Digital hard drive, and his HP USB drive, as well as all derivative fruits thereof.<sup>1</sup>

As reason therefor, defendant states:

1. He had a reasonable expectation of privacy in his ACER laptop, his Western Digital hard drive, and his HP USB drive.
2. These items were seized without a warrant on January 6, 2011.
3. The Secret Service did not obtain a warrant to search these items until February 9, 2011, Exhibit 38, 34 days after their seizure; that warrant was not executed before its expiration, and another warrant was issued on February 24, 2011, Exhibit 29, 49 days after their seizure.
4. The delay in obtaining search warrants for these items rendered their seizure unreasonable under the Fourth Amendment, requiring that all fruits of the searches of those items be suppressed.

---

<sup>1</sup> All averments herein regarding Swartz's ownership and possession of the ACER laptop, the hard drive, and the USB drive are made pursuant to the protections provided by *Simmons v. United States*, 390 U.S. 377, 392-94 (1968).

**THE DEFENDANT REQUESTS A HEARING ON THE WITHIN MOTION.**

**LOCAL RULE 7.1(A)(2) STATEMENT**

The undersigned counsel has conferred with AUSA Stephen Heymann. The government opposes the suppression remedies sought and will respond to defendant's request for a hearing in its response to the motion.

**MEMORANDUM OF LAW**

**I. FACTUAL BACKGROUND.**

The ACER laptop and the hard drive were seized without a warrant on January 6, 2011.<sup>2</sup> Shortly thereafter, Swartz was arrested, and the backpack he was carrying was searched and the USB thumb drive seized. S/A Pickett delayed obtaining warrants to search the three items until February 9, 2011, 34 days after their seizure. Even then, he allowed those warrants to expire without executing them. He again applied for warrants to search the three items on February 24, 2011, when warrants authorizing the search of the items were again issued.

**II. SWARTZ HAD A REASONABLE EXPECTATION OF PRIVACY AND A POSSESSORY INTEREST IN HIS ACER LAPTOP, HIS HARD DRIVE, AND HIS USB DRIVE.**

With respect to Swartz's reasonable expectation of privacy and possessory interest in his ACER laptop and his hard drive, Swartz incorporates by reference herein the discussion in Section II of his Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law and in Section II of his Motion to

---

<sup>2</sup> For a recitation of the facts leading up to the seizure of the laptop and hard drive, *see* Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, and Incorporated Memorandum of Law, Section I.

Suppress All Fruits of Interceptions and Disclosures of Electronic Communications and Other Information by MIT Personnel in Violation of the Fourth Amendment and the Stored Communications Act and Incorporated Memorandum of Law. With respect to the USB drive, it belonged to Swartz and was in his backpack when it was searched incident to his arrest and was seized from him at that time. Accordingly, he plainly had a reasonable expectation of privacy in the drive and its contents and a possessory interest in it which its seizure deprived him of.

### **III. THE DELAY IN OBTAINING A WARRANT RENDERED THE SEIZURE OF THESE ITEMS UNREASONABLE.**

“[E]ven a seizure lawful at its inception can nevertheless violate the Fourth Amendment because its manner of execution infringes possessory interests protected by the Fourth Amendment’s prohibition on ‘unreasonable searches.’” *United States v. Jacobson*, 466 U.S. 109, 124 (1984). *See, e.g., Segura v. United States*, 468 U.S. 796, 812 (1984) (“[A] seizure reasonable at its inception because based on probable cause may become unreasonable as a result of its duration”); *United States v. Burgard*, 675 F.3d 1029, 1032 (7th Cir. 2012)(“When officers fail to seek a search warrant, at some point the delay becomes unreasonable and is actionable under the Fourth Amendment”); *United States v. Mitchell*, 565 F.3d 1347, 1350 (11th Cir. 2009)(“even a seizure based on probable cause is unconstitutional if the police act with unreasonable delay in securing a warrant”); *United States v. Riccio*, 2011 WL 4434855 at \*1 (S.D.Cal. Sept. 23, 2011)(“The finding of probable cause to seize the hard drive did not relieve law enforcement of its obligation to ‘diligently’ obtain a warrant,” quoting *United States v. Dass*, 849 F.3d 414, 415 (9th Cir. 1988)).

After seizing an item without a warrant, an officer must make it a priority to secure a search warrant that complies with the Fourth Amendment. This will entail diligent work to present a warrant application to the judicial officer at the earliest reasonable time.

*Burgard*, 675 F.3d at 1035.

In *Mitchell*, the Eleventh Circuit considered a considerably less extensive delay than that present here in obtaining a warrant for the search of a hard drive – 21 days – and held that, under the circumstances of that case, the delay in obtaining a search warrant was unreasonable, thus violating the Fourth Amendment and requiring the suppression of the fruits of the search of the hard drive. In balancing the defendant’s possessory interest against the government’s interests, the Court first stressed the very strong possessory interests that individuals have in their computers:

Computers are relied upon heavily for personal and business use. Individuals may store personal letters, e-mails, financial information, passwords, family photos, and countless other items of a personal nature on their computer hard drives. Thus, the detention of the hard drive for over three weeks before a warrant was sought constitutes a significant interference with Mitchell’s possessory interests.

565 F.3d at 1351. Weighed against the defendant’s substantial possessory interest, the Court concluded that “there was no compelling justification for the delay.” *Id.* Quite the contrary, the Court concluded: law enforcement authorities simply believed that there was “no rush.” *Id.* at 1353. The Court made a point of noting that the 23-page affidavit submitted in support of the application for the search warrant was largely boilerplate and contained only three double-spaced pages of original content, *id.* at 1351, *i.e.*, the affidavit would not have taken any substantial amount of time to prepare. Other courts have reached similar conclusions. *See, e.g., United States v. Shaw*, 2012 WL 844075 at \*2-\*4 (N.D.Ga. Feb. 10, 2012)(concluding that 90-day delay in obtaining warrant to search seized cell phones was unreasonable under the Fourth Amendment and recommending that evidence obtained from search of cell phones be suppressed), *adopted*, 2012 WL 843919 (N.D.Ga. March 12, 2012); *Riccio*, 2011 WL 4434855 at \*1 (ordering evidence suppressed where law enforcement delayed 91 days in obtaining a warrant to search defendant’s hard drive); *United States*

*v. Rubenstein*, 2010 WL 2723186 at \*13-\*14 (S.D.Fla. June 24, 2010)( recommending suppression of evidence where agents delayed 41 days in obtaining warrant for laptop), *adopted* 2010 WL 2681364 (S.D.Fla. July 7, 2010); *see also United States v. Budd*, 549 F.3d 1140, 1144 (7th Cir. 2008)(assuming without deciding that 48-day delay in obtaining warrant to search computer was unreasonable); *United States v. Kowalczyk*, 2012 WL 3201975 at \*23 (D.Or. Aug. 3, 2012)(terming 7-day delay “unfortunate,” but not finding it unreasonable).

Here, there was a 34-day delay in obtaining the February 9, 2011, warrant, which remained unexecuted, and a total of a 49-day delay until the obtaining of the February 24, 2011, warrant pursuant to which the items were ultimately searched. Swartz had a strong possessory interest in all three items. They belonged to him, and he never voluntarily relinquished his dominion and control over them, nor did he ever consent to their seizure. On the other side of the balance, defendant knows of no conceivable reason which could justify a delay of this magnitude. This was a joint investigation involving the Cambridge Police Department, the United States Secret Service and the MIT Police Department, which was being run by S/A Pickett. *See Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, and Incorporated Memorandum of Law, Sections I, IV.* The affidavit submitted in support of the February 9, 2011, warrant application would have taken very little time to prepare. It was only 11 pages in length, plus two attachments describing the property to be seized, the items to be seized, and the objects of the search.<sup>3</sup> *See Exhibit 32.* The first two pages are largely boilerplate, as are pages 9 and 10. Of the remaining content, that

---

<sup>3</sup> In addition to the three items which are the subject of this motion, the application also sought authorization to search Swartz’s home. That search is the subject of a separate motion to suppress. *See Motion to Suppress All Fruits of Searches Pursuant to a Warrant of 950 Massachusetts Avenue, Apt. 320, Cambridge, Massachusetts, and 124 Mount Auburn Street, Office 504, Cambridge, Massachusetts and Incorporated Memorandum of Law.*

which applies specifically to this case, it is almost entirely a distillation of previously written reports.<sup>4</sup> *See, e.g., Mitchell*, 565 F.3d at 1351 (indicating Court’s belief that 23-page affidavit could have been prepared in the two and a half days before the agent left for two-week training program); *see also Burgard*, 675 F.3d at 1034 (finding it “implausible” that two-page affidavit could not have been prepared in less than six days, particularly as its content was largely derived from previously written reports).

The delay in obtaining the warrants to search the ACER, the hard drive, and the USB drive was unreasonable under the Fourth Amendment. All fruits of the searches of those items must, accordingly, be suppressed.

Respectfully submitted,  
By his attorney,

**/s/ Martin G. Weinberg**  
Martin G. Weinberg  
20 Park Plaza, Suite 1000  
Boston, MA 02116  
(617) 227-3700 (tel.)  
(617) 338-9538 (fax)  
owlmgw@att.net

#### **CERTIFICATE OF SERVICE**

I, Martin G. Weinberg, hereby certify that on this 5th day of October, 2012, a copy of the foregoing document has been served via the Court’s ECF system on all registered participants, including Stephen P. Heymann, AUSA. One copy of the exhibits to the motion has been served on the government by hand this same date.

**/s/ Martin G. Weinberg**

Martin G. Weinberg

---

<sup>4</sup> *See, e.g., Exhibit 15.*

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

_____	)	
UNITED STATES	)	
	)	
v.	)	No. 11-10260-NMG
	)	
AARON SWARTZ	)	
_____	)	

**MOTION TO DISMISS COUNTS 1 AND 2 OF INDICTMENT  
AND INCORPORATED MEMORANDUM OF LAW**

Now comes the defendant Aaron Swartz and respectfully moves that this Honorable Court dismiss Counts 1 and 2 of the indictment.

As reason therefor, defendant states:

1. Counts 1 and 2 charge him with wire fraud in violation of 18 U.S.C. §1343.
2. Section 1343 does not encompass the conduct charged in this case.
3. Section 1343 is void for vagueness in violation of the Due Process Clause as applied to the circumstances of this case.

**THE DEFENDANT REQUESTS A HEARING ON THE WITHIN MOTION.**

**LOCAL RULE 7.1(A)(2) STATEMENT**

The undersigned counsel has conferred with AUSA Stephen Heymann. The government opposes the dismissal remedy sought and will respond to defendant's request for a hearing in its response to the motion.

**MEMORANDUM OF LAW**

Counts 1 and 2 of the indictment charge Swartz with wire fraud in violation of 18 U.S.C. §1343. The indictment alleges that Swartz "having devised and intended to devise a scheme and

artifice to defraud and for obtaining property – journal articles digitized and distributed by JSTOR, and copies of them – by means of material false and fraudulent pretenses and representations, transmitted and caused to be transmitted by means of wire communication in interstate commerce writings, signs, and signals – that is, communications to and from JSTOR’s computer servers – for the purpose of executing the scheme, and aiding and abetting it, including on or about” October 9, 2010, (Count 1) and January 4-6, 2011 (Count 2). Indictment at 10-11, ¶35. Essentially, the indictment alleges that Swartz gained access to the MIT electronic communications network through various mechanisms, and then, having obtained that access, used it to gain access to JSTOR’s website, from which he then downloaded a substantial quantity of digitized journal articles.

**I. SECTION 1343 DOES NOT APPLY TO THE CONDUCT CHARGED IN THIS CASE.**

To convict Swartz of an offense under §1343, the government must prove beyond a reasonable doubt: “[his] knowing and willing participation in a scheme or artifice to defraud with the specific intent to defraud, and (2) the use of . . . interstate wire communications in furtherance of the scheme.” *United States v. Vazquez-Botet*, 532 F.3d 37, 63 (1st Cir. 2008), *quoting United States v. Sawyer*, 85 F.3d 713, 723 (1st Cir. 1996). An essential element of the offense is that the defendant must have made a *material* misrepresentation or omission of fact. *E.g.*, *Neder v. United States*, 527 U.S. 1, 25 (1999); *Mendez Internet Management Services, Inc. v. Banco Santander de Puerto Rico*, 621 F.3d 10, 15 (1st Cir. 2010); *United States v. Blastos*, 258 F.3d 25, 27 (1st Cir. 2001). A misrepresentation or omission is material only if it has “a natural tendency to influence, or is capable of influencing, the decision of the decisionmaking body to which it is addressed.” *United States v. Moran*, 393 F.3d 1, 13 (1st Cir. 2004), *quoting Neder*, 527 U.S. 1, 16. *See, e.g., United*



*States v. Philip Morris USA, Inc.*, 566 F.3d 1095, 1122 (D.C.Cir. 2009)(Materiality requirement is met “if the matter at issue is of importance to a reasonable person making a decision about a particular matter or transaction”); *United States v. Spirk*, 503 F.3d 619, 621 (7th Cir. 2007)(material falsehoods are those “likely to be significant to a reasonable person deciding what to do”); *United States v. Heppner*, 519 F.3d 744, 749 (8th Cir. 2008); *United States v. Lawrence*, 405 F.3d 888, 901 (10th Cir. 2005)(“to determine whether a statement is material the appropriate test is to examine whether it has a natural tendency to influence, or is capable of influencing a decision or action by another”). The first fatal flaw in Counts 1 and 2 is that none of the false statements alleged in the indictment were made to a “decisionmaker” or to person making a decision.<sup>1</sup> Instead, they were uniformly statements to a computer or information passed between computers. The indictment alleges the transmission of the following information:

- that when registering as a guest on the MIT network, Swartz used the fictitious names “Gary Host” and “Grace Host,” each time obtaining a different IP address; Indictment, ¶14(a), 20, 27(a),
- that when registering as a guest on the MIT network, Swartz gave the computer’s client name as “ghost laptop” and “ghost macbook,” Indictment, ¶14(b), 20;
- that when registering as a guest on the MIT network, Swartz provided the email address of “ghost@mailinator.com” and “ghost42@mailinator.com,” Indictment, ¶14(c), 20;
- that, when JSTOR blocked access to the IP address which Swartz’s computer had been using, Swartz established a new IP address which allowed the continued downloading of articles, Indictment, ¶16(b);
- that after MIT blocked access by the computer with the Acer’s MAC address, Swartz twice obtained another guest registration by “spoofing,” *i.e.*, changing, the Acer’s MAC address, again using the name “Gary Host” or “Grace Host” and the client name “ghost laptop,” which led to the laptop’s receiving a new IP address,

---

<sup>1</sup> Many of them were not in fact material false statements of fact at all. *See* Section II, *infra*.

Indictment, ¶¶19(a)-(c), 27(a)-(c);

- that during November-December, 2010, Swartz bypassed the guest registration process by connecting directly to the network and assigning himself two new IP addresses, Indictment, ¶24;
- that Swartz, through the use of MIT IP addresses, made it appear that he was affiliated with MIT, Indictment, ¶34(a);
- that Swartz used an automated collection device which made it appear that multiple people were requesting articles rather than a single person making multiple requests, Indictment, ¶34(c).

This information was all either provided by Swartz or Swartz's laptop to MIT's computer network (name, client name, email address) or was information automatically transmitted from one computer to another (IP addresses, MAC addresses, information about the program running). What is wholly missing here is any person or "decisionmaker" to whom the statements – if they were statements at all – were addressed. There was no person or decisionmaker whose "decision" the information had a tendency to influence or was capable of influencing. Nothing in the wire or mail fraud statutes or the case law construing them suggests that their reach extends to information or statements or omissions which are never reviewed or considered by a human being and do not tend to, nor are they capable of, influencing a decision by person. "Materiality" is an element incorporated directly from common law fraud, *see Neder*, 527 U.S. at 21-25, to which the concepts of machines communicating with each other in the complete absence of human agency and of machines robotically performing various functions would have been utterly foreign and incomprehensible, just as the concept that automatic responses by machines constituted "decisionmaking" would have been.

The rule of lenity precludes stretching the wire fraud statute to reach the conduct charged in this case. The rule of lenity "requires ambiguous criminal laws to be interpreted in favor of the

defendants subjected to them.” *United States v. Santos*, 553 U.S. 507, 2025 (2008). *See United States v. Skilling*, 130 S.Ct. 2896, 2932 (2010)(“[A]mbiguity concerning the ambit of criminal statutes should be resolved in favor of lenity”). Critically, the rule of lenity “ensures fair warning by resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered.” *United States v. Lanier*, 520 U.S. 259, 266 (1997).

In various ways over the years, we have stated that when choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite. . . . This principle is founded on two policies that have long been part of our tradition. First, a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed. To make the warning fair, so fair as possible the line should be clear. . . . Second, because of the seriousness of criminal penalties, and because criminal punishment usually represents the moral condemnation of the community, legislatures and not courts should define criminal activity. This policy embodies the instinctive distastes against men languishing in prison unless the lawmaker has clearly said they should. . . . Thus, where there is ambiguity in a criminal statute, doubts are resolved in favor of the defendant.

*United States v. Bass*, 404 U.S. 336, 347-48 (1971)(internal quotation marks and citations omitted).

Nothing in the wire fraud statute clearly and definitely extends its reach to communications between computers.

In fact, Congress *has* spoken regarding use of computers to commit fraud – but in 18 U.S.C. §1030, not in the wire or mail fraud statutes. Congress’ enactment of §1030(a)(2), criminalizing “intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . [i]nformation from any protected computer” and §1030(a)(4), criminalizing “knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and

obtain[ing] anything of value” – essentially the conduct with which Swartz is charged<sup>2</sup> – provides compelling evidence that it did not believe that such conduct was already encompassed within the reach of the wire fraud statute. Counts 1 and 2 should be dismissed.

## **II. THE STATEMENTS AT ISSUE WERE NOT FALSE STATEMENTS OR MISREPRESENTATIONS OR OMISSIONS OF FACT.**

Swartz’s giving the computer’s client name as “ghost laptop” and “ghost macbook” when registering as a guest on the MIT network,” Indictment, ¶14(b), 20, was not false, and certainly not materially so, because, as the indictment alleges, the client name is one chosen by the user and is simply used to identify the computer on the network. Indictment, ¶14(b). The user is free to choose any name he wishes, and whatever that name is suffices to identify the computer on the network. Here, MIT was always able to identify the computers in use as either “ghost laptop” or “ghost macbook.” The use of those client names was not a fraudulent misrepresentation or omission of material fact.

Similarly, Swartz’s providing the email address of “ghost@mailinator.com” and “ghost42@mailinator.com that when registering as a guest on the MIT network,” Indictment, ¶14(c), 20, was also not the making of a false statement. As the indictment acknowledges, the Mailinator email address was a real one through which Swartz could receive email from MIT if its personnel close to communicate with him. The use of those email addresses was not a fraudulent misrepresentation or omission of material fact.

The establishment of a new IP address, Indictment, ¶16(b), is not the making of a false statement. Indeed, it is not a statement at all. “An IP address is an identifier for a computer or device

---

<sup>2</sup> Swartz is charged with violations of these statutes in Counts 3-12.

on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination.” [http://www.webopedia.com/TERM/I/IP\\_address.html](http://www.webopedia.com/TERM/I/IP_address.html) (last visited October 2, 2012). Thus, an IP address indicates nothing more than the address the computer is using for communications and is, in fact, always true. Swartz made no false statements or misrepresentations or omissions of material fact when he used different IP addresses to access JSTOR. For the same reasons, Swartz’s use of two IP addresses which he allegedly assigned to himself after bypassing the guest registration process and connecting directly to the network, Indictment, ¶¶24, were not false statements or misrepresentations or omissions of material fact. By the same token, obtaining new IP addresses by “spoofing,” *i.e.*, changing, the Acer’s MAC address, Indictment, ¶¶19(a)-(c), 27(a)-(c), also cannot constitute false statements or misrepresentations or omissions of material fact, nor can Swartz’s use of an automated collection device which made it appear that multiple people were requesting articles rather than a single person making multiple requests, Indictment, ¶34(c).

Swartz’s use of MIT IP addresses did not make it appear that he was affiliated with MIT. Indictment, ¶34(a). Instead, MIT had a liberal guest user policy which permitted individuals with no affiliation with MIT whatsoever to access and use the MIT network, *see* Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, and Incorporated Memorandum of Law at 9-10; the use of an MIT IP address did not represent to JSTOR that the person seeking access to its website was affiliated with MIT. This, too, did not constitute a material false statement or misrepresentation or omission of fact.

This leaves only Swartz’s use of fictitious names when registering on MIT’s network as a guest. That statement was made to MIT, not to JSTOR and only allowed Swartz to access the MIT network. It cannot support a charge of devising a scheme to defraud JSTOR of its property, specified

in the indictment as “journal articles digitized and distributed by JSTOR, and copies of them.”

**III. IF §1343 COULD BE APPLIED TO THE CONDUCT CHARGED HERE, IT IS VOID FOR VAGUENESS AS APPLIED TO THIS CASE.**

To pass muster under the Due Process Clause, a statute must give fair warning, “in language that the common world will understand, of what the law intends to do if a certain line is crossed.” *United States v. Hussein*, 351 F.3d 9, 13 (1st Cir. 2003). *See, e.g., United States v. Arcadipane*, 41 F.3d 1, 5 (1st Cir. 1994)(“the Due Process Clause forbids the government from depriving an individual of his liberty unless he is given fair warning of the consequences of that conduct”). “The Due Process Clause demands that criminal statutes describe each particular offense with sufficient definiteness to ‘give a person of ordinary intelligence fair notice that his contemplated conduct is forbidden.’” *Hussein*, 351 F.3d at 13, *quoting United States v. Harriss*, 347 U.S. 612, 617 (1954). *See, e.g., Kolender v. Lawson*, 461 U.S. 352, 357 (1983)(“[A] penal statute [must] define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited” (emphasis added)); *Connally v. General Const. Co.*, 269 U.S. 385, 391 (1926)(“the terms of a penal statute creating a new offense must be sufficiently explicit to inform those who are subject to it what conduct on their part will render them liable to its penalties”(emphasis added)); *United States v. Bohai Trading Co., Inc.*, 45 F.3d 577, 581 (1st Cir. 1995)(issue is “whether the statute, as enacted by Congress, gave sufficient notice that the conduct charged was proscribed” (emphasis added)). In addition, to be valid under the Due Process Clause, penal statutes must be sufficiently specific to prevent arbitrary or discriminatory enforcement. To that end, they must provide comprehensible standards that limit prosecutorial and judicial discretion. *See, e.g., Kolender v. Lawson*, 461 U.S. 352, 357 (1983); *Grayned v. Rockford*, 408 U.S. 104, 108-09 (1972); *Smith v.*

*Goguen*, 415 U.S. 566, 572-73 (1974); *Papachristou v. City of Jacksonville*, 405 U.S. 156, 168 (1972).

As applied to the conduct alleged in this case to have violated §1343, the statute fails to give a person of ordinary intelligence fair notice that conduct such as that charged in this case is forbidden by the statute and could result in criminal prosecution and punishment. Neither the statute, nor any reported judicial decision, “has fairly disclosed” the conduct at issue to be “within [§1343’s] scope.” *Lanier*, 520 U.S. at 266.<sup>3</sup> It may be that the government is seeking to charge a scheme to defraud in

---

<sup>3</sup> This case is not comparable to cases which have applied the wire fraud statute to the distribution and use of devices that enabled users to obtain television or long-distance telephone or internet service without paying for it. *See, e.g., Brandon v. United States*, 382 F.2d 607, 608, 610 (10th Cir.1967)(scheme to defraud telephone company of revenue for the use of long distance telephone service and facilities); *United States v. Manzer*, 69 F.3d 222, 225 (8th Cir.1995)(affirming convictions for wire fraud and mail fraud of a defendant who operated a business whose products enabled users to obtain premium television channels without paying for them); *United States v. Harriss*, 2012 WL 2402788 (D.Mass. June 26, 2012)(upholding against void for vagueness challenge conviction of defendants who sold cable modem hacking products which would permit users to obtain free or higher speed internet access without paying for it); *United States v. Norris*, 833 F.Supp. 1392, 1395-97 (N.D.Ind.1993), *aff’d*, 34 F.3d 530 (7th Cir.1994)(scheme to defraud cable television companies of revenue by selling equipment that allowed individuals to receive premium channels without paying required fee). These cases were held properly prosecuted under the wire fraud statute because the defendants’ products directly enabled their users to defraud the provider of the revenue they would have obtained had the users properly contracted and paid for the services which were instead stolen. Here, in sharp contrast, nothing which Swartz did deprived either MIT or JSTOR of revenue. Guests were entitled to use the MIT network without paying a fee, and, in downloading JSTOR articles, Swartz was not depriving JSTOR of revenue. Moreover, the indictment charges that the property of which JSTOR was defrauded were articles, not revenue.

Nor is this case comparable to *United States v. Czubinski*, 106 F.3d 1069 (1st Cir. 1997), in which an IRS employee accessed and viewed confidential material which was the property of his employer. The Court held that the evidence did not suffice to support the defendant’s conviction for wire fraud, but suggested in dictum that the defendant’s conduct might have violated §1343 had he downloaded the confidential material. That dictum is not binding on this Court. *See, e.g., Fletcher v. Haas*, 851 F.Supp.2d 287, 298 (D.Mass. 2012)(quoting Pierre N. Leval, *Judging Under the Constitution: Dicta About Dicta*, 81 N.Y.U. L.Rev. 1249, 1250 (2006)(noting that when judges accept dictum as if it were binding law, they “fail to discharge [their] responsibility to deliberate on and decide the question which needs to be decided”). Moreover, Swartz had no comparable fiduciary duty to JSTOR, the entity from which the articles were downloaded.

the complete absence of material misrepresentations and omissions. However, “the settled meaning of the term ‘fraud’ at common law required misrepresentation or concealment of a material fact.” *United States v. Harriss*, 2012 WL 2402788 at \*4 (D. Mass. June 26, 2012), *citing Neder*, 527 U.S. at 20-25. Nothing in the wire fraud statute or the cases construing it provides constitutionally adequate notice that manipulating IP addresses, spoofing MAC addresses, and gaining access to a free electronic communications network (MIT’s) for the purpose of accessing another website to download journal articles which are free to those with access to the website, and for which access MIT had already paid, constitutes a federal wire fraud felony carrying a potential penalty of 30 years. Defendant’s research has located no reported wire fraud case which is even remotely comparable to this one. Prosecution of Swartz under §1343 on the theory advanced by the government here would violate Swartz’s rights to due process of law. The number of articles downloaded by Swartz may have exceeded JSTOR’s terms of service, but the wire fraud statute does not exist to police violations of private contracts. Section 1343 is void for vagueness as applied to this case.

Respectfully submitted,  
By his attorney,

**/s/ Martin G. Weinberg**  
Martin G. Weinberg  
20 Park Plaza, Suite 1000  
Boston, MA 02116  
(617) 227-3700 (tel.)  
(617) 338-9538 (fax)  
owlmgw@att.net



**CERTIFICATE OF SERVICE**

I, Martin G. Weinberg, hereby certify that on this 5th day of October, 2012, a copy of the foregoing document has been served via the Court's ECF system on all registered participants, including Stephen P. Heymann, AUSA.

**/s/ Martin G. Weinberg**

Martin G. Weinberg

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4589893@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Notice requesting courtesy copy  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 10/5/2012 at 1:54 PM EDT and filed on 10/5/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** 65(No document attached)

**Docket Text:**

**ELECTRONIC NOTICE issued requesting courtesy copy for [63] MOTION to Suppress , [61] MOTION to Suppress , [62] MOTION to Suppress , [64] MOTION to Dismiss , [59] MOTION to Suppress , [60] MOTION to Suppress as to Aaron Swartz Counsel who filed these documents are requested to submit a courtesy copy of them to the Clerk's Office. These documents must be clearly marked as a Courtesy Copy and reflect the document number assigned by CM/ECF. (Patch, Christine)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4593943@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Order on Motion to Seal  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 10/10/2012 at 11:55 AM EDT and filed on 10/10/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** 67(No document attached)

**Docket Text:**

**Judge Nathaniel M. Gorton: ELECTRONIC ORDER entered granting [66] Motion to Seal as to Aaron Swartz (1) (Patch, Christine)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

**UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS**

**CLERK'S NOTICE**

The image of this document is not viewable because it is either  
SEALED or filed EX PARTE.

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS**

UNITED STATES OF AMERICA,  
  
Plaintiff,

v.

AARON SWARTZ,  
  
Defendant.

Crim. No. 11-CR-10260-NMG

**NOTICE OF APPEARANCE FOR DEFENDANT AARON SWARTZ**

PLEASE TAKE NOTICE that Matthias Kamber of the law firm of Keker & Van Nest LLP, 633 Battery Street, San Francisco, CA 94111, Telephone (415) 391-5400, Fax (415) 397-7188, email: mkamber@kvn.com is entering his appearance as counsel of record for Defendant Aaron Swartz in the above-captioned matter.

The above-named attorney has registered for the Court's Electronic Court Filing ("ECF") in the above-captioned matter. Copies of all pleadings and notices pertaining to the above-captioned matter not otherwise filed through the Court's ECF system should henceforth be served upon him at the following address:

Matthias Kamber  
Keker & Van Nest LLP  
633 Battery Street  
San Francisco, CA 94111  
Tel: 415-391-5400  
Fax: 415-397-7188  
Email: mkamber@kvn.com

As soon as the requisite certificates of good standing can be obtained from the California State Bar, motions for admission *pro hac vice* for Keker & Van Nest lawyers Elliot R. Peters, Daniel Purcell and Cody S. Harris will be filed with the Court pursuant to Local Rule 83.5.3. Subject to the Court granting those motions, it is anticipated that Mr. Peters will be lead counsel

for Mr. Swartz going forward. Requests to the California State Bar to obtain these certificates have been submitted on an expedited basis. Counsel are aware that motions in the above-captioned matter are pending and a trial date has been set. They further understand that Martin Weinberg, Esq. will be withdrawing as counsel. They seek no alteration of the present schedule due to this substitution of counsel.

Dated: October 31, 2012

Respectfully submitted,

/s/ Matthias Kamber

MATTHIAS KAMBER (MA 654217)

KEKER & VAN NEST LLP

633 Battery Street

San Francisco, CA 94111-1809

415 391 5400 (Telephone)

415 397 7188 (Facsimile)

Attorneys for Defendant AARON SWARTZ

**CERTIFICATE OF SERVICE**

I, Matthias Kamber, hereby certify that on this date, October 31, 2012, a copy of the foregoing document has been served via CM/ECF Electronic Filing, upon Assistant U.S.

Attorney Steven P. Heymann.

/s/ Matthias Kamber

Matthias Kamber

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

_____	)	
UNITED STATES OF AMERICA	)	
	)	
	)	
v.	)	Criminal No. 11-10260-NMG
	)	
	)	
AARON SWARTZ	)	
	)	
_____	)	

**MOTION FOR LEAVE TO WITHDRAW AS COUNSEL**

Now comes Martin G. Weinberg who hereby moves, pursuant to Rule 83.5.2(c) of the Local Rules of the District of Massachusetts, to withdraw as counsel for the defendant Aaron Swartz for the following reason: the defendant has retained the law firm of Kecker and Van Nest of San Francisco, California, as his new counsel and that members of that firm are filing Notices of Appearances and, at least as to Elliot Peters Esq., a request for Pro Hac Vice. Although a trial date has been set for February, 2013, and a schedule for the filing of motions and expert disclosures (and other discovery obligations) has been set, successor counsel (if this motion is allowed) will inform the Court that they will seek admittance subject to the current trial and pretrial schedule.

Respectfully submitted,

**/s/ Martin G. Weinberg**  
Martin G. Weinberg, Esq.  
Mass. Bar No. 519480  
20 Park Plaza, Suite 1000  
Boston, MA 02116  
Telephone: (617) 227-3700  
Facsimile: (617) 338-9538  
[owlmgw@att.net](mailto:owlmgw@att.net)

**Certificate of Service**

I, Martin G. Weinberg, hereby certify that on this date, October 31, 2012, a copy of the foregoing document has been served via CM/ECF upon all registered parties including Assistant U.S. Attorney Stephen Heymann. The forgoing document has also been served upon Aaron Swartz via electronic mail.

**/s/Martin G. Weinberg**  
Martin G. Weinberg, Esq.

Date: October 31, 2012



MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4626057@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Order on Motion to Withdraw as Attorney  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 11/1/2012 at 1:16 PM EDT and filed on 11/1/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** 71(No document attached)

**Docket Text:**

**Judge Nathaniel M. Gorton: ELECTRONIC ORDER entered granting [70] Motion to Withdraw as Attorney Attorney Martin G. Weinberg terminated as to Aaron Swartz (1) (Patch, Christine)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Martin G. Weinberg owlmc@att.net, owlmgw@att.net

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Matthias A. Kamber mkamber@kvn.com, ashen@kvn.com, plemos@kvn.com

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 11-10260-NMG
	)	
AARON SWARTZ,	)	
	)	
Defendant	)	

AGREED-UPON MOTION RE BRIEFING

The parties have conferred about several matters concerning Defendant Swartz's motions to suppress and to dismiss. The Government has briefed responses to these motions, but will require an extra four days to finish them and file them. In addition, rather than file five separate responses to the five separate motions to suppress, the Government proposes to file one consolidated response, which, because it would answer so many motions, would be longer than the page limits set by the local rules. Defendant Swartz would like permission to file a reply brief, and to have that brief be due on December 3, 2012.

The parties agree with each others' requests, and therefore move the Court to order that the deadline for the Government to file its responses to the motions to suppress and dismiss be continued from November 13, 2012, to November 16, 2012; that the Government's consolidated brief in response to the motions to suppress may exceed the page limits set by the local rules; and

that Defendant Swartz be allowed to file a reply brief no later than December 3, 2012.

Respectfully submitted,

Carmen M. Ortiz  
United States Attorney

By: /s/ Scott L. Garland  
STEPHEN P. HEYMANN  
SCOTT L. GARLAND  
Assistant U.S. Attorneys

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants identified on the Notice of Electronic Filing.

/s/ Scott L. Garland  
SCOTT L. GARLAND  
Assistant United States Attorney

Date: November 8, 2012

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA,  
  
Plaintiff,

v.

AARON SWARTZ,  
  
Defendant.

Crim. No. 11-CR-10260-NMG

**NOTICE OF APPEARANCE FOR DEFENDANT AARON SWARTZ**

PLEASE TAKE NOTICE that Michael J. Pineault of the law firm of Clements & Pineault, LLP, 24 Federal Street, Boston, MA 02110, Telephone No. 857 445 0135, Facsimile No. 857 366 5404, email: [mpineault@clementspineault.com](mailto:mpineault@clementspineault.com) is entering his appearance as counsel of record for Defendant Aaron Swartz in the above-captioned matter.

The above-named attorney has registered for the Court's Electronic Court Filing ("ECF") in the above-captioned matter. Copies of all pleadings and notices pertaining to the above-captioned matter not otherwise filed through the Court's ECF system should henceforth be served upon him at the following address:

Michael J. Pineault  
Clements & Pineault, LLP  
24 Federal Street  
Boston, MA 02110  
Tel.: (857) 445-0135  
Fax: (857) 366-5404  
Email: [mpineault@clementspineault.com](mailto:mpineault@clementspineault.com)

Motions for admission *pro hac vice* for Keker & Van Nest LLP lawyers Elliot R. Peters and Daniel Purcell will be filed with the Court pursuant to Local Rule 83.5.3. Subject to the Court granting those motions, it is anticipated that Mr. Peters will be lead counsel for Mr. Swartz

going forward. Counsel are aware that motions in the above-captioned matter are pending and a trial date has been set. They further understand that Martin Weinberg, Esq. will be withdrawing as counsel. They seek no alteration of the present schedule due to this substitution of counsel.

Dated: November 8, 2012

Respectfully submitted,

/s/ Michael J. Pineault

Michael J. Pineault  
Clements & Pineault, LLP  
24 Federal Street  
Boston, MA 02110  
Tel.: (857) 445-0135  
Fax: (857) 366-5404  
Email: [mpineault@clementspineault.com](mailto:mpineault@clementspineault.com)

Attorneys for Defendant AARON SWARTZ

**CERTIFICATE OF SERVICE**

I, Michael J. Pineault hereby certify that on this date, November 8, 2012, a copy of the foregoing document has been served via CM/ECF Electronic Filing, upon Assistant U.S.

Attorney Steven P. Heymann.

/s/ Michael J. Pineault

Michael J. Pineault

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS**

UNITED STATES OF AMERICA,  
  
Plaintiff,

v.

AARON SWARTZ,  
  
Defendant.

Crim. No. 11-CR-10260-NMG

**MOTION OF DEFENDANT**

**TO ADMIT ELLIOT R. PETERS *PRO HAC VICE***

In accordance with Local Rule 83.5.3(b), through the undersigned attorney duly admitted to practice before this Court, the defendant hereby moves that Elliot R. Peters be permitted to represent him in the above captioned action for all matters related to this case.

In support of this motion, the undersigned states:

1. Elliot R. Peters is an attorney with the law firm of Keker & Van Nest, LLP, 633 Battery Street, San Francisco, California 94111-1809.
2. Elliot R. Peters is admitted to practice before the State Bar of California (California State Bar No. 158708), United States District Court, Northern District of California and United States Court of Appeals for the Ninth Circuit.
3. Pursuant to Local Rule 85.5.3, a Certificate setting forth the necessary information for the admission of Elliot R. Peters *pro hac vice* is submitted herewith as Exhibit A. The email address of Mr. Peters is as follows:  
  

[epeters@kvn.com](mailto:epeters@kvn.com)
4. The undersigned member of this Bar has agreed to act as local counsel for the above-listed defendant in this proceeding and, as such, agrees to be the recipient of all pleadings

and communications on behalf of the above-listed defendants. The address and telephone number to which all such pleadings and communications may be sent are as follows:

Keker & Van Nest LLP  
633 Battery Street  
San Francisco, CA 94111-1809

Wherefore, the undersigned respectfully requests that this Court admit Elliot R. Peters *pro hac vice* to practice as a visiting attorney before this Court representing the above-listed defendants in all matters related to this proceeding. The appropriate admission fee in the amount of \$100.00 has been paid. A [Proposed] Order is attached hereto.

LOCAL RULE 7.1(A)(2) CERTIFICATION

Pursuant to Local Rule 7.1(A)(2), counsel for the above-listed defendants has conferred with counsel for plaintiff regarding this motion. Counsel for plaintiff has ASSENTED to the allowance of this motion.

Dated: November 8, 2012

Respectfully submitted,

/s/ Michael J. Pineault

Michael J. Pineault  
Clements & Pineault, LLP  
24 Federal Street  
Boston, MA 02110  
Tel.: (857) 445-0135  
Fax: (857) 366-5404  
Email: [mpineault@clementspineault.com](mailto:mpineault@clementspineault.com)

Attorneys for Defendant AARON SWARTZ

**CERTIFICATE OF SERVICE**

I, Michael J. Pineault, hereby certify that on this date, November 8, 2012, a copy of the foregoing document has been served via CM/ECF Electronic Filing, upon Assistant U.S.

Attorney Steven P. Heymann.

/s/ Michael J. Pineault  
Michael J. Pineault



# EXHIBIT A

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS**

UNITED STATES OF AMERICA,  
  
Plaintiff,

v.

AARON SWARTZ,  
  
Defendant.

Crim. No. 11-CR-10260-NMG

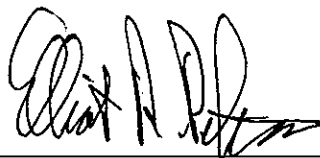
**LOCAL RULE 83.5.3(B) CERTIFICATE**

**OF ELLIOT R. PETERS**

I, Elliot R. Peters, am a partner in the firm of Kecker & Van Nest, 633 Battery Street, San Francisco, California 94111, counsel to the defendant in this action, hereby certify that:

1. I am a member in good standing of the Bar of the State of California.
2. There are no disciplinary proceedings pending against me as a member of the Bar of the State of California.
3. I am familiar with the Local Rules of the United States District Court for the District of Massachusetts.

Dated: November 8, 2012



\_\_\_\_\_  
Elliot R. Peters



## THE STATE BAR OF CALIFORNIA

180 HOWARD STREET, SAN FRANCISCO, CALIFORNIA 94105-1617

TELEPHONE: 888-800-3400

### CERTIFICATE OF STANDING

October 30, 2012

#### TO WHOM IT MAY CONCERN:

This is to certify that according to the records of the State Bar, ELLIOT REMSEN PETERS, #158708 was admitted to the practice of law in this state by the Supreme Court of California on June 10, 1992; and has been since that date, and is at date hereof, an ACTIVE member of the State Bar of California; and that no recommendation for discipline for professional or other misconduct has ever been made by the Board of Trustees or a Disciplinary Board to the Supreme Court of the State of California.

THE STATE BAR OF CALIFORNIA

A handwritten signature in black ink, appearing to read "Louise Turner".

Louise Turner  
Custodian of Membership Records

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA,

Plaintiff,

v.

AARON SWARTZ,

Defendant.

Crim. No. 11-CR-10260-NMG

**[PROPOSED] ORDER FOR ADMISSION *PRO HAC VICE***

The Court has reviewed the Motion of Defendant Aaron Swartz to Admit Elliot R. Peters  
*Pro Hac Vice*.

Upon consideration of that motion, the Court grants attorney Elliot R. Peters *pro hac vice*  
admission to this Court

Dated: \_\_\_\_\_

\_\_\_\_\_  
Honorable Nathaniel M. Gorton  
United States District Judge

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS**

UNITED STATES OF AMERICA,  
  
Plaintiff,

v.

AARON SWARTZ,  
  
Defendant.

Crim. No. 11-CR-10260-NMG

**MOTION OF DEFENDANT**

**TO ADMIT DANIEL E. PURCELL *PRO HAC VICE***

In accordance with Local Rule 83.5.3(b), through the undersigned attorney duly admitted to practice before this Court, the defendant hereby moves that Daniel Purcell be permitted to represent him in the above captioned action for all matters related to this case.

In support of this motion, the undersigned states:

1. Daniel Purcell is an attorney with the law firm of Keker & Van Nest, LLP, 633 Battery Street, San Francisco, California 94111-1809.
2. Daniel Purcell is admitted to practice before the State Bar of California (California State Bar No. 191424), United States District Court, Northern District of California and United States Court of Appeals for the Ninth Circuit.
3. Pursuant to Local Rule 85.5.3, a Certificate setting forth the necessary information for the admission of Daniel Purcell *pro hac vice* is submitted herewith as Exhibit A. The email address of Mr. Purcell is as follows:  

[dpurcell@kvn.com](mailto:dpurcell@kvn.com)
4. The undersigned member of this Bar has agreed to act as local counsel for the above-listed defendant in this proceeding and, as such, agrees to be the recipient of all pleadings

and communications on behalf of the above-listed defendants. The address and telephone number to which all such pleadings and communications may be sent are as follows:

Keker & Van Nest LLP  
633 Battery Street  
San Francisco, CA 94111-1809

Wherefore, the undersigned respectfully requests that this Court admit Daniel Purcell *pro hac vice* to practice as a visiting attorney before this Court representing the above-listed defendants in all matters related to this proceeding. The appropriate admission fee in the amount of \$100.00 has been paid. A [Proposed] Order is attached hereto.

LOCAL RULE 7.1(A)(2) CERTIFICATION

Pursuant to Local Rule 7.1(A)(2), counsel for the above-listed defendants has conferred with counsel for plaintiff regarding this motion. Counsel for plaintiff has ASSENTED to the allowance of this motion.

Dated: November 8, 2012

Respectfully submitted,

/s/ Michael J. Pineault

Michael J. Pineault  
Clements & Pineault, LLP  
24 Federal Street  
Boston, MA 02110  
Tel.: (857) 445-0135  
Fax: (857) 366-5404  
Email: [mpineault@clementspineault.com](mailto:mpineault@clementspineault.com)

Attorneys for Defendant AARON SWARTZ

**CERTIFICATE OF SERVICE**

I, Michael J. Pineault, hereby certify that on this date, November 8, 2012, a copy of the foregoing document has been served via CM/ECF Electronic Filing, upon Assistant U.S.

Attorney Steven P. Heymann.

/s/ Michael J. Pineault  
Michael J. Pineault

# EXHIBIT A



**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS**

UNITED STATES OF AMERICA,  
  
Plaintiff,

v.

AARON SWARTZ,  
  
Defendant.

Crim. No. 11-CR-10260-NMG

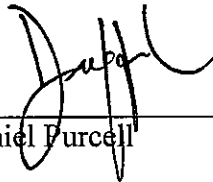
**LOCAL RULE 83.5.3(B) CERTIFICATE**

**OF DANIEL E. PURCELL**

I, Daniel Purcell, am a partner in the firm of Keker & Van Nest, 633 Battery Street, San Francisco, California 94111, counsel to the defendant in this action, hereby certify that:

1. I am a member in good standing of the Bar of the State of California.
2. There are no disciplinary proceedings pending against me as a member of the Bar of the State of California.
3. I am familiar with the Local Rules of the United States District Court for the District of Massachusetts.

Dated: November 8, 2012

  
\_\_\_\_\_  
Daniel Purcell



## THE STATE BAR OF CALIFORNIA

180 HOWARD STREET, SAN FRANCISCO, CALIFORNIA 94105-1617

TELEPHONE: 888-800-3400

### CERTIFICATE OF STANDING

October 30, 2012

#### TO WHOM IT MAY CONCERN:

This is to certify that according to the records of the State Bar, DANIEL EDWARD PURCELL, #191424 was admitted to the practice of law in this state by the Supreme Court of California on December 9, 1997; and has been since that date, and is at date hereof, an ACTIVE member of the State Bar of California; and that no recommendation for discipline for professional or other misconduct has ever been made by the Board of Trustees or a Disciplinary Board to the Supreme Court of the State of California.

THE STATE BAR OF CALIFORNIA

A handwritten signature in cursive script, appearing to read "Louise Turner".

Louise Turner  
Custodian of Membership Records

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS**

UNITED STATES OF AMERICA,  
  
Plaintiff,

v.

AARON SWARTZ,  
  
Defendant.

Crim. No. 11-CR-10260-NMG

**[PROPOSED] ORDER FOR ADMISSION *PRO HAC VICE***

The Court has reviewed the Motion of Defendant Aaron Swartz to Admit Daniel Purcell *Pro Hac Vice*.

Upon consideration of that motion, the Court grants attorney Daniel Purcell *pro hac vice* admission to this Court

Dated: \_\_\_\_\_

\_\_\_\_\_  
Honorable Nathaniel M. Gorton  
United States District Judge

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4637429@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Order on Motion for Leave to Appear  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 11/9/2012 at 11:11 AM EST and filed on 11/9/2012

**Case Name:** USA v. Swartz  
**Case Number:** 1:11-cr-10260-NMG  
**Filer:**  
**Document Number:** 76(No document attached)

**Docket Text:**

**Judge Nathaniel M. Gorton: ELECTRONIC ORDER entered granting [74] Motion for Leave to Appear Pro Hac Vice Added Elliot R. Peters. Attorneys admitted Pro Hac Vice must register for electronic filing if the attorney does not already have an ECF account in this district. To register go to the Court website at [www.mad.uscourts.gov](http://www.mad.uscourts.gov). Select Case Information, then Electronic Filing (CM/ECF) and go to the CM/ECF Registration Form. as to Aaron Swartz (1); granting [75] Motion for Leave to Appear Pro Hac Vice Added Daniel E. Purcell. Attorneys admitted Pro Hac Vice must register for electronic filing if the attorney does not already have an ECF account in this district. To register go to the Court website at [www.mad.uscourts.gov](http://www.mad.uscourts.gov). Select Case Information, then Electronic Filing (CM/ECF) and go to the CM/ECF Registration Form. as to Aaron Swartz (1) (Moore, Kellyann)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Stephen P. Heymann [Stephen.Heymann@usdoj.gov](mailto:Stephen.Heymann@usdoj.gov), [Jodi.gird@usdoj.gov](mailto:Jodi.gird@usdoj.gov), [usama.ecf@usdoj.gov](mailto:usama.ecf@usdoj.gov)

Michael J. Pineault [mpineault@clementspineault.com](mailto:mpineault@clementspineault.com)

Scott Garland [scott.garland@usdoj.gov](mailto:scott.garland@usdoj.gov), [jodi.gird@usdoj.gov](mailto:jodi.gird@usdoj.gov), [usama.ecf@usdoj.gov](mailto:usama.ecf@usdoj.gov)

Matthias A. Kamber [mkamber@kvn.com](mailto:mkamber@kvn.com), [ashen@kvn.com](mailto:ashen@kvn.com), [plemos@kvn.com](mailto:plemos@kvn.com)

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

Daniel E. Purcell  
Keker & Van Nest, LLP  
633 Battery Street  
San Francisco, CA 94111-1809

Elliot R. Peters

Keker & Van Nest  
633 Battery Street  
San Francisco, CA 94111

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4639933@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Order on Motion for Miscellaneous Relief  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 11/13/2012 at 9:49 AM EST and filed on 11/13/2012

**Case Name:** USA v. Swartz  
**Case Number:** 1:11-cr-10260-NMG  
**Filer:**  
**Document Number:** 77(No document attached)

**Docket Text:**

**Judge Nathaniel M. Gorton: ELECTRONIC ORDER entered granting in part and denying in part [72] Assented to MOTION Extension of Response Brief Deadline, Permission to File Response Brief Exceeding Local Rule's Page Limits, and Filing a Reply Brief as to Aaron Swartz by USA. "The Government may file a consolidated brief in opposition to defendant's motions to suppress and it may do so by November 16. Defendant is granted leave to file a reply brief by December 3. The Government's consolidated brief, however, may not exceed 55 pages and the Defendant's reply is not to exceed 10 pages." (Moore, Kellyann)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Michael J. Pineault mpineault@clementspineault.com

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Matthias A. Kamber mkamber@kvn.com, ashen@kvn.com, plemos@kvn.com

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

Daniel E. Purcell  
Keker & Van Nest, LLP  
633 Battery Street  
San Francisco, CA 94111-1809

Elliot R. Peters  
Keker & Van Nest  
633 Battery Street  
San Francisco, CA 94111

**UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS**

<b>UNITED STATES OF AMERICA</b>	)	
	)	
v.	)	<b>Criminal No. 11-10260-NMG</b>
	)	
<b>AARON SWARTZ,</b>	)	
	)	
<b>Defendant</b>	)	

**GOVERNMENT’S CONSOLIDATED RESPONSE TO  
DEFENDANT’S MOTIONS TO SUPPRESS**

The Court should deny Defendant Aaron Swartz’s five motions to suppress (Dkt. Nos 59-63), which attack the manner in which the Government collected the vast majority of electronic and physical evidence in this case.

**I. INTRODUCTION**

**A. The Victims: JSTOR and MIT**

A research or university library can find the cost and space to maintain a comprehensive collection of academic journals extraordinarily expensive. Founded in 1995, JSTOR is an independent, self-sustaining, non-profit organization that provides research and university libraries access to numerous academic journals without the normal costs of a paper-based collection. To do so, JSTOR digitizes articles and distributes them over an online system that it built, which enables libraries to outsource the journals’ storage, ensures their preservation, and enables them to be searched extensively by authorized users.

JSTOR pays copyright-holders for permission to digitize the copyright-holders’ articles and make them available online.<sup>1</sup> To pay its expenses, JSTOR normally charges subscription

---

<sup>1</sup> Some materials available on JSTOR are not subject to copyright.

fees to its customers. For this access, a large research library might pay JSTOR more than \$50,000 a year. In addition, JSTOR also charges customers for access to certain individual journal articles on an article-by-article fee. JSTOR shares portions of its fees with the articles' and journals' copyright-holders.

As at any library, users of JSTOR are to access articles a few at a time as they need them for their research. JSTOR employs computerized methods to track and limit its users' downloading activity. In addition to these computerized methods, before a legitimate user can download an article from JSTOR, the user is prompted to review and accept JSTOR's terms of service. (Ex. 1). Each article downloaded from JSTOR also comes with a cover page confirming the user's acceptance of the terms of service and a link to the location where the terms are found. (Ex. 2). The terms of service, commonsensibly, state that you cannot use automated computer programs to systematically download and export content from JSTOR's archive. (Ex. 3). The user prompt, cover sheet, and terms of service emphasize that you cannot download an entire issue of a journal without prior permission. (Exs. 1-3).

The Massachusetts Institute of Technology ("MIT") is a renowned scientific research university. When a guest registers his computer on MIT's computer network, he must agree to follow the same computer rules of use that the faculty, students and employees must follow. These rules of use require that the guest's activities on MIT's network be consistent with the network's purpose of supporting research, education and MIT administrative activities. In return, MIT assigns the guest an IP address<sup>2</sup> and allows the guest computer network service for a

---

<sup>2</sup>An IP (Internet protocol) address is like a telephone number for a computer. Each computer attached to the Internet must be assigned an IP address so the computer's incoming and outgoing Internet traffic can be directed properly from the traffic's source to its destination. An



short period, only 14 days per year. (Ex. 4). As configured during the events alleged in the Superseding Indictment, a guest whom MIT had granted an IP address could request and receive digitized journal articles from JSTOR.

### **B. The Defendant: Aaron Swartz**

During the period alleged in the Superseding Indictment, Aaron Swartz was a fellow at Harvard University's Safra Center for Ethics, on whose website he was described as a "writer, hacker and activist." Harvard provided Swartz with access to JSTOR's services and archives as needed for his research there. Swartz was not a student, faculty member, or employee of MIT. In the Guerilla Open Access Manifesto, which Swartz actively participated in drafting and had posted on one of his websites, Swartz advocated "tak[ing] information, wherever it is stored, mak[ing] our copies and shar[ing] them with the world." (Ex. 5).

### **C. Overview of the Offenses**

Between September 24, 2010 and January 6, 2011, Swartz schemed to (a) break into a restricted-access network wiring closet at MIT; (b) attach his computer to a network switch within that closet and thus access MIT's computer network; (c) use MIT's computer network to access JSTOR's archive of digitized journal articles; (d) download a substantial portion of JSTOR's archive onto his computer and computer hard drives, which at times impaired the operation of JSTOR's computers and resulted in MIT's loss of JSTOR access; (e) avoid MIT's and JSTOR's efforts to prevent this type of massive copying, efforts that were directed at users

---

IP address consists of a unique series of four numbers, each ranging from 0-225, separated by periods (*e.g.*, 18.55.7.216). For example, when a user types in the District Court's website address as "www.mad.uscourts.gov", his computer network translates that phrase into the website hosting computer's IP address, 199.107.17.221, to direct his communications to the site.

generally and at Swartz specifically; and (f) elude detection and identification.

## **II. THE FACTS**

Late during the night of September 24, 2010, an individual registered his computer on MIT's campus and obtained a guest account on MIT's computer network. The individual did not provide his true identity at this or any subsequent time, and neither MIT personnel nor law enforcement officers knew the individual's name until his arrest months later. The individual registered his computer by specifying his name as "Gary Host," a pseudonym, and his e-mail address as ghost@mailinator.com, a disposable e-mail address by virtue of its requiring no initial e-mail registration and keeping no records of e-mail access.<sup>3</sup> Before assigning the computer an IP address, MIT's network automatically collected the computer's owner-created name — "ghost laptop" — and the unique identifying number associated with the computer's Internet networking hardware, known as the computer's Media Access Control or "MAC" address. These are standard login and communication procedures.

MIT's DHCP<sup>4</sup> computer server then used a standard Internet protocol to assign the individual an IP address (18.55.6.215) for use while on the network. The network kept records of the computer's registration information, its IP address, and its MAC address. These records are standard computer-networking records, and did not include any computer commands that the individual typed in or ran, or any data that the computer downloaded. (Exs. 6, 7).

---

<sup>3</sup> Mailinator advertised itself as a free e-mail service that would accept mail for any e-mail address directed to mailinator.com without need for a prior registration or account; would automatically delete all e-mail after several hours, whether read or not; and would keep no logs (records) of e-mail access.

<sup>4</sup> DHCP is the acronym for Dynamic Host Configuration Protocol.

On September 25, 2010, the day after registering the “ghost laptop,” the individual used the “ghost laptop” to systematically access and rapidly download an extraordinary volume of articles from JSTOR by using a software program that sidestepped JSTOR’s computerized limits on the volume of each user’s downloads. The downloads and requests for downloads were so numerous, rapid, and massive that they impaired the performance of JSTOR’s computers.

As JSTOR, and then MIT, became aware of these downloads and problems, both attempted to block the individual’s computer from further communications. On the evening of September 25, 2010, after suffering hundreds of thousands of downloads from the ghost laptop, JSTOR temporarily ended the downloads by blocking network access from the computer at IP address 18.55.6.215.

The next day, however, the ghost laptop’s user obtained a new IP address from MIT’s network, changing the last digit in its IP address by one from 18.55.6.215 to 18.55.6.216. This defeated JSTOR’s IP address block, enabling the ghost laptop to resume furiously downloading articles from JSTOR. This downloading continued until the middle of September 26, when JSTOR spotted it and blocked communication from IP address 18.55.6.216 as well.

The September 25 and 26 downloads had impaired JSTOR’s computers and misappropriated significant portions of its archive. Because the download requests had originated from two MIT IP addresses that had begun with 18.55.6 — that is, 18.55.6.215 and 18.55.6.216 — JSTOR began blocking a broader range of MIT IP addresses on September 26. The new block prevented MIT researchers assigned MIT IP addresses 18.55.6.0 through 18.55.6.255 (as many as 253 computers) from performing research through JSTOR’s archive for three to four days.

Moreover, when JSTOR notified MIT of the problems, MIT, too, banned the “ghost laptop” from using its network. To do this, MIT terminated the ghost laptop’s guest registration on September 27, 2010, and prohibited the computer, as identified by its hardware MAC address, from being assigned a new IP address again through the guest registration process.

On October 2, 2010, less than a week after JSTOR and MIT had barred the individual’s ghost laptop from communicating with their networks, the individual obtained yet another guest connection for the ghost laptop on MIT’s network. Having recognized that MIT or JSTOR had blocked his ghost laptop by recognizing its MAC address, the individual now manipulated the ghost laptop’s MAC address to mislead MIT into believing that he was a new and different guest registrant.<sup>5</sup>

Six days later, the individual connected a second computer to MIT’s network and created another guest account using pseudonyms similar to those he had used with the “ghost laptop”: he registered the new computer under the name “Grace Host”, a temporary email address of ghost42@mailinator.com, and a computer client name of “ghost macbook.”

On October 9, 2010, the individual activated the ghost laptop and the ghost macbook to download JSTOR’s articles once again. The downloads came so fast and numerous that the individual again significantly impaired the operation of some of JSTOR’s computers.

Once again, MIT could not identify who was controlling these computers or where they were physically located, and JSTOR could not isolate the interloper to a consistent IP address

---

<sup>5</sup> A computer’s MAC address is initially assigned by an equipment manufacturer, but can be misrepresented electronically by a knowledgeable user. The user altered the ghost laptop’s MAC address to appear as 00:23:5a:73:5f:fc rather than the prior MAC address of 00:23:5a:73:5f:fb.

that could be blocked. Consequently, JSTOR blocked access by *every* computer using an MIT IP address campus-wide for approximately three days, again depriving legitimate MIT users from accessing JSTOR's services. And MIT blocked computers using the ghost laptop's and the ghost macbook's MAC addresses as well.

Nevertheless, between the end of October and January 6, 2011, the hacker obtained at least three new IP addresses and assigned his computer two new MAC addresses. He also moderated the speed of the downloads, which made them less noticeable to JSTOR. The exfiltration of JSTOR's collection was nonetheless extreme: over this period, the individual downloaded well over a million of JSTOR's articles.

Because the hacker had modified the speed of his downloads, JSTOR did not notice his latest downloads until around Christmas, 2010. Once noticed, however, JSTOR provided MIT with the hacker's latest IP address. Now that MIT's network security personnel had a more robust set of network tools, they could consult network traffic routing records and trace the IP address back to a concrete physical location on campus.

So on January 4, 2011, an MIT network security analyst traced the hacker's IP address to a network switch located in a basement wiring closet in MIT's Building 16. Building 16's street-level doors have no-trespassing signs posted on them. (Ex. 8). The wiring closet is protected by a pair of locked steel doors. (Ex. 9). The closet is generally locked, but at that time its lock could be forced by a quick jerk of its double doors. When MIT personnel entered the closet, they found a cardboard box with a wire leading from it to a computer network switch. (Ex. 10).<sup>6</sup>

---

<sup>6</sup> MIT personnel removed the box from the laptop at first, and then MIT personnel or law enforcement officers replaced the box on one or more occasions. The second photograph was taken after the box was replaced, not when it was initially found.

Hidden under the box was the ghost laptop, an Acer-brand laptop, connected to a separate hard drive for excess storage. (Ex. 11). The network cable connected the laptop to the network switch, thus giving the laptop Internet access. (Ex. 12). The laptop's direct connection to the network switch was unusual because MIT does not connect computers directly to those switches.

MIT called campus police to the scene, who, in turn, brought in the Cambridge Police and the Secret Service. Over the course of the morning and early afternoon of January 4th, MIT and law enforcement officers collaboratively<sup>7</sup> took several steps to identify the perpetrator and learn what he was up to:

- (1) Cambridge Police crime scene specialists fingerprinted the laptop's interior and exterior and the external hard drive and its enclosure;
- (2) MIT placed and operated a video camera inside the closet, which, as discussed below, later recorded the hacker (subsequently identified as Aaron Swartz) entering the wiring closet and performing tasks within it;
- (3) The Secret Service opened the laptop and sought to make a copy of its volatile memory (RAM), which would automatically be destroyed when the laptop's power was turned off, but the effort resulted in their seeing only the laptop's user sign-in screen;
- (4) MIT connected a second laptop to the network switch in order to record the laptop's communications, a type of recording often referred to as a "packet capture;" the Secret Service subsequently concurred with the packet capture, none of which was turned over to officers until MIT was issued a subpoena after Swartz's arrest;<sup>8</sup>
- (5) Beginning on January 4, 2011, MIT agreed to provide, and later provided, the Secret Service copies of network logs pertaining to

---

<sup>7</sup> From the time of law enforcement's arrival on January 4, 2011, through the suspect's arrest and identification on January 6, 2011, the effort by MIT and law enforcement to identify the individual was both consensual and collaborative.

<sup>8</sup> This second laptop is seen on a chair in Ex. 10.

the ghost laptop and ghost macbook between September 24, 2010 and January 6, 2011, some of which records were provided consensually, the remainder of which were provided pursuant to a subpoena to MIT.<sup>9</sup>

By mid-day on January 4th, MIT and law enforcement personnel had completed their initial crime scene investigation. Experience told them that merely removing the hacker's computer equipment would just result in his renewing his efforts elsewhere. So, rather than take the hacker's equipment away, MIT and law enforcement instead restored the closet to its initial appearance upon discovery, and monitored who entered it and handled the laptop. In this way, the hacker would not necessarily know that his criminal tools had been discovered, his identity might be uncovered, and he could be stopped.

The ruse worked. Within an hour of their departure, the hacker returned. After entering the wiring closet and shutting the doors behind him, (Ex. 13), the hacker replaced the hard drive connected to the laptop with a new one he took from his backpack, and then concealed his equipment once again underneath the cardboard box.

Two days later, on January 6, 2011, the hacker returned to the wiring closet yet again. This time, worried about being identified, the hacker covered his face with his bicycle helmet as he entered the closet. (Ex. 14). Once inside and with the door closed, the hacker disconnected the laptop and placed it, the external hard drive, and the network cable in his backpack. (Ex. 15). As he left, he again hid his face with his bicycle helmet. (Ex. 16).

By January 6, 2011, the hacker had downloaded a major portion of the 6 to 7 million articles then contained in JSTOR's digitized database.

---

<sup>9</sup> As discussed below, both the law and MIT's policies and procedures allowed MIT to turn these records over consensually, but it also could, and at points did, insist upon a subpoena.

A little after 2:00 that afternoon, MIT Police Captain Albert Pierce, who had been involved in the investigation, was heading down Massachusetts Avenue within a mile of MIT when he spotted a bicyclist who looked like the hacker caught on the wiring closet video. Captain Pierce identified himself as a police officer. After a brief exchange, the individual dropped his bike to the ground and ran away. The individual was chased, apprehended, arrested, and identified as Aaron Swartz. During a search incident to arrest, Cambridge police found a USB storage drive in Swartz's backpack, which they seized and stored as evidence.

Approximately an hour later, MIT technical staff used computer routing and addressing records to locate Swartz's ghost laptop and hard drive in the Student Information Processing Board's office in MIT's student center. Law enforcement found the equipment on the floor under a desk. (Ex. 17). The equipment was subsequently seized and stored as evidence by Cambridge Police.

Aaron Swartz was charged by the Commonwealth in a criminal complaint alleging breaking and entering into MIT's property with intent to commit a felony, and was subsequently indicted by a Massachusetts grand jury for the same charge along with stealing JSTOR's electronically processed or stored data, and accessing a computer system without authorization.

While the Commonwealth pursued state charges, the U.S. Attorney's Office began a separate investigation on January 5, 2011. On February 9, 2011, the Secret Service obtained a warrant to search Swartz's apartment, followed by a warrant to search his office on February 11, 2011. Both were executed on February 11th. Also on February 9, 2011, the Secret Service obtained warrants to seize from the Cambridge Police and then search the laptop, the hard drive, and the USB storage device. These warrants were returned unexecuted and new warrants were



obtained on February 24, 2011. On May 16, 2011, Swartz was served with a forfeiture warrant for property of JSTOR in his possession and refused to comply with the Court's warrant.<sup>10</sup>

Swartz was indicted federally for wire fraud, computer fraud, and data theft, which was followed by the present Superseding Indictment on the same theories.

### **III. MOTION TO SUPPRESS INTERCEPTIONS AND DISCLOSURES OF ELECTRONIC COMMUNICATIONS BY MIT PERSONNEL (No. 1)<sup>11</sup>**

Swartz first moves to suppress: (1) the historical guest registration, DHCP and IP address assignment and network routing records that MIT collected independently before January 4th as it sought to identify and locate the hacker; (2) the recording (or "packet capture") of the laptop's communications after it was found connected to MIT's network; and (3) the network's historical routing, addressing and switching records used to find the laptop after Swartz relocated it from Building 16 to the student center (Building W20) just before his arrest.

Apparently without a trace of irony, Swartz argues that MIT and law enforcement violated his rights to privacy as he hid his computers and hard drives in MIT's locked wiring closet, used pseudonyms to avoid identification, hard-wired his computers to MIT's network switch to avoid detection, siphoned off JSTOR's copyrighted documents, kept reconfiguring his computer to circumvent MIT's and JSTOR's efforts to keep him off their networks, and relocated the evidence to MIT's student center. In particular, Swartz asserts that the evidence listed above should be suppressed because the Wiretap Act, 18 U.S.C. § 2510 *et seq.*, the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, and the Fourth Amendment prevented MIT and

---

<sup>10</sup> Swartz later reached a civil agreement with JSTOR, pursuant to which he delivered to the Secret Service four hard drives containing millions of JSTOR's documents.

<sup>11</sup> Swartz's numbering convention is used here for ease of reference.

law enforcement from taking natural investigative steps to find his equipment and identify him.

The motion should be denied on several independent and self-supporting grounds. Swartz lacked a reasonable expectation of privacy in MIT's business records. As a trespasser, Swartz lacked a reasonable expectation of privacy on MIT's computer network. The Wiretap Act offers no suppression remedy for electronic communications (as opposed to oral or wire communications), and the Stored Communications Act offers no suppression remedy whatsoever. Even if the Wiretap Act offered a suppression remedy for electronic communications, MIT's network routing, addressing and switching records were not electronic communications under the statute.

As a preliminary matter, Swartz's motion should be denied to the extent that he seeks to suppress any actions taken before January 4, 2011, because neither local nor federal law enforcement officers were investigating Swartz's downloading activity before January 4, 2011, when MIT first found the laptop. None of MIT's and JSTOR's private investigative steps before then can be attributed to the Government for the purpose of Fourth Amendment or statutory analysis, and the results of any private search before January 4, 2011, cannot be suppressed.

**A. Routing, Addressing and Switching Information from MIT's Computer Network**

**1. *Swartz Lacked a Constitutionally-Protected Reasonable Expectation of Privacy in MIT's Network Records***

Nearly any attorney involved in the criminal justice system can recite by heart the "reasonable expectation of privacy" test for determining whether government activity constitutes a search cognizable by the Fourth Amendment. Under *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J. concurring), the warrant requirement is implicated only if (1) the individual exhibited an actual (subjective) expectation of privacy, and (2) society is prepared to recognize

this expectation as (objectively) reasonable.

Swartz did not exhibit an actual, subjective expectation of privacy in MIT's network records. He has not submitted an affidavit declaring that he did. Nor could he credibly do so. Swartz is an experienced software engineer,<sup>12</sup> and thus understood that when he connected to MIT's and JSTOR's networks, his computer would send the networks his IP and MAC address information and that they would likely store that information as well.<sup>13</sup> In fact, Swartz demonstrated his subjective knowledge that MIT and JSTOR would record this information: when JSTOR blocked communications from Swartz's IP address, he changed his IP address by a single digit, and when MIT blocked his MAC address from obtaining a guest registration, he changed that by a single letter. And Swartz used a duplicitous name and email address when he sought a guest registration. He used and changed these identifiers precisely because he knew that his computer would disclose this type of information to MIT and JSTOR and that their networks would routinely log and record it.

Even if Swartz had truly believed that MIT would keep its computer records private, that expectation would not be "one that society is prepared to recognize as 'reasonable.'" *Smith v. Maryland*, 442 U.S. 735, 743 (1979) (quoting *Katz*, 389 U.S. at 361). In *Smith*, the Supreme Court concluded that neither installing nor using a pen register to collect information about the numbers dialed from the petitioner's home telephone constituted a search under the Fourth Amendment. In concluding that it did not constitute a search, the Supreme Court reasoned first

---

<sup>12</sup> See <http://en.wikipedia.org/wiki/Aaron-Swartz> (last visited Oct. 23, 2012) for his background.

<sup>13</sup> Indeed, MIT's IS&T (Information Services and Technology) DHCP Usage Logs Policy, quoted by Swartz at p. 7 of his motion, provided further notice that IP address, MAC address, and other information would be collected by the network. (Ex. 18).

that the petitioner could not have held any subjective expectation of privacy in the numbers that he had dialed because he knew that these numbers would be disclosed to a third party, the telephone company. *Id.* at 742. Even were this not the case, as the Supreme Court explained,

This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties. In [*U.S. v. Miller*, 425 U.S. 435 (1976)], for example, the Court held that a bank depositor has no “legitimate ‘expectation of privacy’” in financial information “voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business.”

. . . .

This analysis dictates that petitioner can claim no legitimate expectation of privacy here. When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and “exposed” that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed. The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber.

*Id.* at 743-44 (citations omitted).

Just as in *Smith*, when Swartz used his computer, he knowingly and voluntarily gave information to a third party, MIT, so that electronic communications could be routed to and from his computer. This computer addressing, routing and switching information is merely the Internet equivalent of telephone numbering, cabling and subscriber information. When using MIT’s network, Swartz assumed the risk that MIT would reveal this network connectivity information – which contained no substantive content<sup>14</sup> – to the police.

This was the conclusion in *United States v. Forrester*, 495 F.3d 1041 (9th Cir. 2007),

---

<sup>14</sup> Swartz claims that these records included the content of his communications, but that is easily disproved by reviewing the records, excerpted in Exs. 6-7. If you liken computer communications to documents sent via FedEx, these records disclose information about the envelope and the delivery tracking information you can see online, not the contents of the documents inside.

which ruled that law enforcement's discovery of Internet e-mail and IP addressing information is outside the scope of the Fourth Amendment. The court reasoned:

[E]mail and Internet users, like the telephone users in *Smith*, rely on third-party equipment in order to engage in communications. *Smith* based its holding that telephone users have no expectation of privacy in the numbers they dial on [sic] the users' imputed knowledge that their calls are completed through telephone switching equipment. Analogously, e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of their websites they visited because they should know that these IP addresses are sent and these IP addresses are accessed through the equipment of their Internet service provider and other third parties. Communication by both Internet and telephone requires people to "voluntarily turn[ ] over [information] to third parties."

495 F.3d at 1048-49 (citations omitted). Other appellate courts have reached the same conclusion. See *U.S. v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010) (holding defendant lacked reasonable expectation of privacy in his IP address because it is conveyed to and from third parties); *United State v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) (holding that "subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation" because it is voluntarily conveyed to third parties); *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010) (holding defendant identified no "evidence that he had a subjective expectation of privacy in his internet . . . 'subscriber information'" because he "voluntarily conveyed" that information to the company, and "assumed the risk" that the company would provide that information to the police (internal citations omitted)); *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001) ("We conclude that plaintiffs . . . lack a Fourth Amendment privacy interest in their subscriber information because they communicated it to the system's operators.").

Despite all these cases, Swartz urges that even if he lacked a reasonable expectation of privacy in other network addressing, routing and switching records, he had a reasonable expectation of privacy in the IP address that MIT gave him. In this regard, he invites the Court

to stretch the law of cell phone tracking to IP addresses, on the ground that MIT had configured its network so that knowing a computer's IP address would identify which campus building housed the computer. There is, however, no reasonable expectation of privacy in an IP address. *See Forrester*, 495 F.3d at 1048-49; *Christie*, 624 F.3d at 573-74. Further, even were the analogy apt, courts, including Judge Stearns in this District, have held that the Fourth Amendment does not protect *historical* cell tower location records. *In re Applications*, 509 F. Supp. 2d 76 (D. Mass. 2007) (Stearns, D.J.).<sup>15</sup> Here, MIT examined only historical IP records. So even were the cell phone analogy apt, it would not bolster Swartz's constitutional claim.

Swartz argues that MIT's policies created a reasonable expectation of privacy in MIT's DHCP logs. He has not averred, nor could he credibly aver, that he looked up and read MIT's written policy on DHCP log disclosure before he pseudonymously obtained a guest registration on their network. Without reading them, they could not create an expectation of any form on his part. Further, even if Swartz had read the policy, he would have read its warning that MIT might *disclose* the logs in compliance with a court order or a valid subpoena. The policy does not promise to disclose records *only* under those circumstances. Swartz cannot turn a warning that records might be disclosed to law enforcement into a guarantee of privacy.

---

<sup>15</sup> *See also, e.g., United States v. Dye*, 2011 WL 1595255, at \*9 (N.D. Ohio Apr. 27, 2011) (denying motion to suppress historical cell data); *United States v. Velasquez*, 2010 WL 4286276, at \*5 (N.D. Cal. Oct. 22, 2010) (same); *United States v. Benford*, 2010 WL 1266507, at \*3 (N.D. Ind. Mar. 26, 2010); *United States v. Suarez-Blanca*, 2008 WL 4200156, at \*8-\*11 (N.D. Ga. Mar. 26, 2008) (same); *Mitchell v. States*, 25 So. 3d 632, 635 (Fla. Dist. Ct. App. 2009) (same). *But see In re Application of the United States*, 620 F.3d 313, 317 (3d Cir. 2010) (asserting location information is not voluntarily conveyed to a cell phone provider but historical cell site records are "obtainable under a § 2703(d) order and that such an order does not require a traditional probable cause determination"); *In Re Application of the United States*, 809 F. Supp. 2d 113, 122-25 (E.D.N.Y. 2011); *In re Application of the United States*, 747 F. Supp. 2d 827 (S.D. Tex. 2010), *appeal docketed*, No. 11-20884 (5th Cir. Dec. 12, 2011).

**2. *Neither MIT Nor the Government Violated the Wiretap or Stored Communication Act By Collecting Non-Content Network Addressing, Routing and Switching Records***

As alternative bases for suppression, Swartz argues that MIT violated the Wiretap Act and that the Government and MIT both violated the Stored Communications Act.

*a. No Statutory Suppression Remedies*

These statutory arguments fail from the outset because even had MIT or the Government violated these acts, neither act contains a suppression remedy for this type of case. Under the Wiretap Act, Congress provided a suppression remedy for violations involving wire and oral communications, but not those involving electronic communications, which are at issue here.<sup>16</sup> *See United States v. Meriwether*, 917 F.2d 955, 960 (6th Cir. 1990); *United States v. Reed*, 575 F.3d 900, 915 (9th Cir. 2009); *United States v. Amanuel*, 615 F.3d 117, 125 (2d Cir. 2010). Meanwhile, Congress determined that suppression was inappropriate for violations of the Stored Communications Act under *all* circumstances. 18 U.S.C. § 2708; Wayne R. LaFare, Jerold H. Israel, Nancy J. King, and Orin S. Kerr, *Criminal Procedure* § 4.8(F) (3d ed. 2011) (“Importantly, the Stored Communications Act does not include a statutory suppression remedy for the unlawful acquisition or disclosure of records of the contents of communications, whether they are wire or electronic communications.”). *See also, e.g., U.S. v. Perrine*, 518 F.3d at 1202; *United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998).

With no suppression remedies, the motion to suppress must be denied.

---

<sup>16</sup> While wire and electronic communications may both be transmitted by wire, “wire communications” by definition convey a human voice, while “electronic communications” do not. *See* 18 U.S.C. § 2510 (1), (12), (18). None of the communications that Swartz seeks to suppress were spoken; all, accordingly, were electronic communications.

*b. No Violation of the Wiretap Act*

Even if the Acts theoretically allowed suppression, suppression would still be inappropriate because neither MIT nor the Government violated the Acts. MIT did not violate Title III by collecting routing and switching information in its network or by giving the Government historical network records that contained no “content.” Title III prohibits the “interception” of oral, wire, and electronic communications. *See* 18 U.S.C. § 2510(1), (2), (4), (12). “Intercept” is defined as the “acquisition of the *contents* of any wire, electronic, or oral communication.” § 2510(4) (emphasis added). “Contents” include only “information concerning the substance, purport, or meaning of that communication.” § 2510(8). MIT did not violate the Wiretap Act in collecting logging records quite simply because the logs contain no “substance, purport or meaning” of Swartz’s communications. Consider again excerpts from the guest registration, DHCP, and radius logs attached at Exs. 6-7. As is evident from the face of these mindless and frequently repetitive records, they do not contain any communications’ contents. Rather, returning to the FedEx metaphor, these records contain information about the envelope, not the documents inside.

Swartz misreads *In re Application for an Order Authorizing use of a Pen Register and Trap*, 396 F. Supp. 2d 45 (D. Mass. 2005) (Collings, M.J.), to claim that “dialing, routing, addressing, and signaling information” regarding communications must also include the communications’ contents. What Magistrate Judge Collings said is that “dialing, routing, addressing, and signaling information” concerning an Internet communication *might* contain the communication’s contents if the information included an e-mail’s subject line, a Google search’s query terms, requested file names, or file paths. *See id.* at 48-49. What Magistrate Judge Collings also said is that if none of that information is included within the “dialing, routing,



addressing, and signaling information,” then that information does not constitute contents. *Id.* Because the records included in Exs. 6-7 do not contain requests to JSTOR for its files, responses from JSTOR, or requests to websites such as Google for information, those records do not include contents and thus their disclosure could not violate the Wiretap Act.

*c. No Violation of the Stored Communications Act*

Nor did the Government violate the Stored Communications Act by obtaining MIT’s historical network records without a warrant. The Stored Communications Act prohibits a provider of “electronic communication service to the public” from “divulg[ing] a record or other information pertaining to a subscriber to or customer of such service” to the government except “as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service.” 18 U.S.C. § 2702(a)(3), (c)(3). Because of these qualifications, the Stored Communications Act simply did not apply.

*i. No service to “the public”*

To begin with, the Stored Communications Act does not apply to MIT because MIT does not provide an “electronic communication service *to the public*.” *See generally* 18 U.S.C. § 2702 (emphasis added) (limiting voluntary disclosure of information by a provider of “electronic communication service to the public”). “The word ‘public’ . . . is unambiguous. Public means the ‘aggregate of the citizens’ or ‘everybody’ or ‘the people at large’ or ‘the community at large.’ *Black’s Law Dictionary* 1227 (6th ed. 1990).” *Anderson Consulting LLP v. UOP*, 991 F. Supp. 1041-42 (N.D. Ill. 1998) (interpreting Stored Communications Act, sometimes referred to as the Electronic Communications Privacy Act). “Thus the statute covers in it any entity that provides electronic communications (e.g., e-mail) service to the community at large.” *Id.*

But MIT does not provide its computer services to the “aggregate of the citizens,”

“everybody,” “the people at large,” or “the community at large.” Rather, MIT restricts use of its computer network to people who support MIT-sanctioned research and educational activities:

MIT’s computing and network facilities and services are to be used for Institute purposes only and not for the benefit of private individuals or other organizations without authorization. Unauthorized access to the use of MIT computer and network services violates this policy.

See MIT’s Policy on the Use of Information Technology ¶ 13.2.3 (Ex. 22). This policy is reiterated in MIT’s Rules of Use of the network, which states that:

The purpose of MITnet is to support research, education, and MIT administrative activities, by providing access to computing resources and the opportunity for collaborative work. All use of the MIT network must be consistent with this purpose.

(Ex. 4, § 1). These restrictions — which Swartz ignored during his crime and again in his brief — matter a great deal. “Providers do not provide services to the public if a person needs a special relationship with the provider to obtain an account.” Wayne LaFare, Jerold Israel, Nancy King and Orin Kerr, *Principles of Criminal Procedure: Investigation*, § 3.11(e) (2d ed. 2009) (interpreting Stored Communications Act). Because MIT provided its network for the use of MIT’s students, faculty and employees and their on-campus guests working with them on MIT-related pursuits, and MIT did not provide its network to everybody in Cambridge, MIT did not provide an “electronic communication service to the public.” Consequently, MIT’s disposition of its records does not fall under the Stored Communications Act.

*ii. Swartz was not MIT’s “customer” or “subscriber”*

The Stored Communications Act is also inapplicable because Swartz was not MIT’s customer or subscriber. The Act’s restrictions on a provider of electronic communications services to the public from disclosing its communication records to law enforcement protect only the provider’s “subscriber[s] or customer[s].” See 18 U.S.C. § 2702(a)(3). But Swartz was not

MIT's subscriber or customer. Swartz was not working on an MIT-related endeavor and instead gave MIT multiple false identities and identifiers. To call him MIT's subscriber or customer would be to call a shoplifter a "customer" or an airplane stowaway a "passenger."

Swartz says that he was MIT's subscriber or customer because MIT personnel repeatedly referred in internal and external communications to the hacker who was exfiltrating JSTOR's archive as a "guest." While MIT did refer to the hacker as a "guest," Swartz attributes too much to this usage. MIT referred to the hacker as a guest in order to identify the *type of account* that Swartz was using, not to verify that they had extended him an invitation.<sup>17</sup> Indeed, throughout this period no one even knew who "Gary Host" or "Grace Host" were, and no MIT personnel had "invited" Swartz to meet in MIT's restricted wiring closet or invited him to connect directly to MIT's network switch. The term "guest" was being used simply in contradistinction to an identifiable faculty member, student or employee. Consequently, Swartz was not a protected "subscriber" or "customer" under the statute and he cannot claim the statute's protections.

Even if Swartz could somehow claim to have been MIT's subscriber or customer when he first registered his computer on September 24, 2010, he lost that status on September 27, 2010, after the first two large download incidents, when MIT banned his network access through the MAC address block. And Swartz lost it again when MIT banned him again on October 13, 2010.

*iii. Proper disclosures to protect MIT's rights and property*

Finally, even if MIT had been a provider "to the public" and even if Swartz had been MIT's subscriber or customer, MIT properly complied with the Stored Communications Act by

---

<sup>17</sup> Nor could Swartz claim that MIT's e-mails to JSTOR misled him into thinking that he was a guest, since he was not a party to those e-mails.

providing the Government records in order to protect its rights by locating and identifying the hacker. Under the Stored Communications Act, MIT could lawfully disclose the necessary records as “necessarily incident to the rendition of the [electronic communications] service or to the protection of the rights or property of the provider of that service.” 18 U.S.C. § 2702(c)(3). Disclosures by service providers such as MIT are held to the standard of reasonableness. *See United States v. Harvey*, 540 F.2d 1345, 1350 (8th Cir. 1976) (interpreting similar language in the wiretap statute found at 18 U.S.C. § 2511 (2)(a)(i)).

MIT wanted to rid its network of Swartz, or else MIT would not have banned his MAC addresses and installed a videocamera in his hiding place. And MIT had good reasons to rid itself of Swartz: his actions had resulted in MIT’s JSTOR service being shut off and MIT researchers’ being denied access to research materials. Thus, MIT was protecting not just JSTOR’s rights, as Swartz claims, but also MIT’s own rights in its network, its interest in using that network to provide its researchers JSTOR articles, and its contract with JSTOR to provide JSTOR’s articles over its network. Under § 2702(a)(3), MIT’s disclosures were proper.

Swartz argues that MIT’s disclosure of network records to law enforcement under § 2703(c)(3) was not “necessarily incident” to protecting MIT’s network because MIT could have protected itself simply by removing his computer from the wiring closet. But MIT had no such assurance. The hacker had repeatedly re-accessed the network after direct efforts to stop him. As far as MIT knew, taking away his computer would merely spur him to return with more equipment yet again. Instead, MIT had to identify the hacker and assist with his apprehension in order to prevent further abuse. Providing the Government these records was necessarily incident

to identifying the hacker and thus protecting MIT's rights and property under § 2703(c)(3).<sup>18</sup>

Consequently, MIT acted properly when it disclosed these records to law enforcement both consensually at the outset and later pursuant to a subpoena.

### **B. The Packet Capture of the Laptop's Communications<sup>19</sup>**

Unlike the other records that Swartz's first motion attempts to suppress, the packet capture of the laptop's communications did involve intercepting the communications' contents. Unlike the system logs discussed above, intercepting the contents of electronic communications usually requires a Title III order, absent an exception.

There is an applicable exception here, however, because Swartz was a trespasser on MIT's system during the packet capture on January 4th. As a matter of constitutional law, a trespasser lacks a reasonable expectation of privacy in a place he has no legitimate right to be. *Rakas v. Illinois*, 439 U.S. 128, 143-44, n.12 (1978) (no legitimate expectation of privacy where a person's presence is wrongful); *United States v. Curlin*, 638 F.3d 562, 565 (7th Cir. 2011) (defendant had no reasonable expectation of privacy in house from which he had been

---

<sup>18</sup> Swartz also contends that MIT's disclosure of its routing and trafficking records violated his Fourth Amendment rights, citing *Crispin v. Christian Audigler, Inc.* 717 F. Supp. 2d 965 (C.D. Cal. 2010); and *In re United States*, 665 F. Supp. 2d 1210 (D. Or. 2009). These cases are inapposite because they did not consider the application of § 2702(c)(3). However, even if MIT had violated the Stored Communications Act by providing the Government its historical routing and registration records without a warrant, doing so would not have rendered the Government's acquisition of those records a *per se* unreasonable search under the Fourth Amendment. See *City of Ontario California v. Quon*, 130 S. Ct. 2619, 2632 (2010) ("Respondents point to no authority for the proposition that the existence of statutory protection [under the Stored Communications Act] renders a search *per se* unreasonable under the Fourth Amendment. And the precedents counsel otherwise.").

<sup>19</sup> No derivative use has been made of this packet capture, and at the present time, the Government does not intend to introduce it in its case-in-chief. The Government responds, however, to preserve its right to use this evidence should it become material.

evicted); *United States v. Sanchez*, 635 F.2d 47, 64 (2d Cir. 1980) (“[A] mere trespasser has no Fourth Amendment protection in a premises he occupies wrongfully.”); *Amezquita v. Hernandez-Colon*, 518 F.2d 8, 11 (1st Cir. 1975) (squatters formerly evicted from public land had no expectation of privacy in homes they unlawfully constructed there); *United States v. Gale*, 136 F.3d 192, 195 (D.C. Cir. 1998) (individual lacked legitimate expectation of privacy in apartment he occupied without permission of its tenant or other legal authority); *United States v. Rambo*, 789 F.2d 1289, 1295-95 (8th Cir. 1986) (hotel occupant asked to leave by police officers acting for hotel management no longer had a reasonable expectation of privacy in hotel room).

Swartz was a trespasser in every sense of the word. To physically get to the network he passed doors with “no trespassing” signs, went into a basement corridor and opened locked steel doors to hide in a restricted wiring closet. Then, having accessed the network using pseudonyms, Swartz repeatedly manipulated his computer’s MAC address as MIT repeatedly barred its use on their network. As a trespasser, then, Swartz had no constitutional expectation of privacy in the electronic communications being sent to and from his computer in the wiring closet.

Title III integrates the constitutional trespasser exception in a statutory exception to its order requirement:

- (i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer if –
  - (I) the owner or operator of the protected computer authorizes the interception of the computer trespasser’s communications on the protected computer;
  - (II) the person acting under color of law is lawfully engaged in

an investigation;

- (III) the person acting under the color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and
- (IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

18 U.S.C. § 2511(2)(i).<sup>20</sup>

The packet capture here fits the statutory exception. First, MIT authorized it. § 2511(2)(i)(I). Second, the packet capture was performed by “a person acting under color of law engaged in an investigation,” § 2511(2)(i)(II); although MIT personnel initiated the packet capture, law enforcement investigators called to the scene concurred that it should continue. Third, MIT and law enforcement investigators “had reasonable grounds to believe that the contents of the computer trespasser's communications w[ould] be relevant to the investigation,” § 2511(2)(i)(III), by helping to identify who owned the ghost laptop and what unlawful activities the computer was conducting on the network. Finally, the packet capture was set up so that it

---

<sup>20</sup> Swartz's Wiretap Act argument in Motion to Suppress No. 1 analyzes a different exception, the provider exception set forth in 18 U.S.C. § 2511(2)(a)(i). *See* Def.'s Motion to Suppress No. 1 at 8-14. That analysis centers on Swartz's misguided notion that MIT acted only to protect JSTOR, and not itself, as well. As discussed above in the context of the Stored Communications Act, *supra* at 22-23, this is incorrect: MIT was not just protecting JSTOR's rights, but also MIT's own rights in its network and in its contract with JSTOR to provide JSTOR's articles over MIT's network. Accordingly, for the same reasons articulated *supra* at 22-23, MIT had the right to intercept and disclose to law enforcement the communications over its network to and from the ghost laptop to protect MIT's rights and property. 18 U.S.C. § 2511(2)(a)(i). Swartz's objection to using the provider exception should be overruled.

Swartz analyzes the Wiretap Act's trespasser exception, 18 U.S.C. § 2511(2)(i), in his Motion to Suppress No. 2 at 17-18.

“d[id] not acquire communications other than those transmitted to or from the computer trespasser.” § 2511(2)(i)(IV).

Here, too, Swartz unsuccessfully seeks to paint himself as MIT’s guest rather than as its computer trespasser. See Def.’s Motion to Suppress No. 2 at 17-18. A “computer trespasser” is “a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer,” 18 U.S.C. § 2510(21)(A), and “does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer,” § 2510(21)(B). Again, it is disingenuous for Swartz to claim that he was MIT’s invitee after MIT had repeatedly cut off his computer’s connection. Neither Swartz’s ability to fake his way onto the system nor MIT’s referring to his logon account as a guest turned him into an invitee. *See supra* at 21-22 (discussing MIT’s and JSTOR’s efforts to ban Swartz). Certainly he was not “a person known by the owner or operator of [MIT’s network] to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.” § 2510(21)(B).

Accordingly, MIT and the Government met each of the elements of § 2511(i)’s trespasser exception to the wiretap order and a Title III order was not necessary to monitor the ghost laptop’s communications.

#### **IV. MOTION TO SUPPRESS FRUITS OF WARRANTLESS SEARCHES (No. 2)**

After MIT tracked the JSTOR downloads to the laptop in the closet, MIT called the police. When the Cambridge Police and Secret Service arrived, they processed the scene for



fingerprints and unsuccessfully attempted to copy volatile evidence in the computer's random access memory ("RAM") which would be destroyed if the computer were turned off.

Swartz's Motion to Suppress No. 2 moves to suppress the fruits of each of these investigative steps.<sup>21</sup> This motion is meritless and should be denied. Swartz lacked a reasonable expectation of privacy in equipment hidden on somebody else's property. The officers were lawfully in MIT's wiring closet, where the laptop and hard drive were in plain view. Exigent circumstances justified the attempt to capture the contents of the laptop's RAM before it was powered down. In any event, this aspect of Swartz's motion is moot because law enforcement officers were unable to copy the RAM.

**A. Swartz Lacked a Reasonable Expectation of Privacy in MIT's Wiring Closet and Student Center Office and the Things He Hid There**

Swartz lacked a reasonable expectation of privacy in the laptop and hard drives that he hid in MIT's wiring closet and student center office. He placed the computer where he and it had no right to be, and left the equipment unattended for extended periods while it robotically stole massive portions of JSTOR's database. The equipment was an instrumentality of a crime, being used in an ongoing crime, when crime scene investigators opened the laptop and hard drive cases on January 4, 2011 and seized them on January 6, 2011.

***1. Whatever Swartz's Claimed Subjective Expectation of Privacy in Instrumentalities of Ongoing Crime Hidden in a Victim's Locked Utility Closet and Office, It is Not One That Society is Objectively Prepared to Recognize***

Whatever subjective expectation of privacy Swartz may have had by using bogus

---

<sup>21</sup> Motion to Suppress No. 2 also seeks again to suppress the results of the packet capture. Those arguments are dealt with in the Government's response to Motion to Suppress No. 1.

identifiers on the laptop, hiding it with a hard drive in a wiring closet that MIT restricted from the public by lock, key and steel doors, concealing the equipment from MIT staff and employees under a cardboard box, and moving it to under a desk in an office in the student center to avoid detection, that expectation was not an objectively reasonable one that society is prepared to accept and adopt. *See Katz*, 389 U.S. at 361. Just because you can freely walk across MIT's campus and sit in its lobbies and you can freely walk into this courthouse and sit in a courtroom, it does not follow that you can enter either facility's locked basement wiring closet. And just because you can freely walk into MIT's library or the First Circuit's library here does not mean that you are free to return whenever you want after being forcibly removed for stealing.

Investigating a crime scene for ephemeral forensic evidence before it is disturbed is fundamental to conducting a criminal investigation, both to identify suspects and eliminate those who might otherwise be wrongfully accused. The recognized need for this is nowhere more clear than when what is being examined are concealed instrumentalities of an ongoing crime.

**2. *A Person Whose Presence Is "Wrongful" Has No Legitimate Expectation of Privacy in Things Wrongfully Stored on a Third-Party's Premises***

Swartz lacked a reasonable expectation of privacy in the wiring closet and its contents and in the office in the student center and its contents. As the First Circuit has noted, "[a]t least three cases have held that a guest in a hotel or motel room loses his reasonable expectation of privacy when his rental period has elapsed. A fortiori, one who occupied the room by just inviting himself in could create for himself no reasonable expectation of privacy." *Amezquita v. Hernandez-Colon*, 518 F.2d 8, 11 (1st Cir. 1975) (citations omitted). Here, Swartz "occupied the room by just inviting himself in," and therefore "could create for himself no reasonable

expectation of privacy.” *Id.*

Like a “burglar plying his trade in a summer cabin during the off season,” Swartz’s presence was “wrongful,” and consequently any subjective expectation of privacy he may have had would not be “one that society is prepared to recognize as ‘reasonable.’” *Rakas v. Illinois*, 439 U.S. 128, 143-44, n.12 (1978) (citations omitted). “[I]ndividuals who occupy a piece of property unlawfully have no claim under the Fourth Amendment.” *United States v. Curlin*, 638 F.3d 562, 565 (7th Cir. 2011) (holding that evicted tenant who remained in house had no legitimate expectation of privacy in house, bedroom in house, or closet in bedroom). Because Swartz had no legitimate expectation of privacy in MIT’s basement wiring closet or student center office, no Fourth Amendment search occurred in either place.<sup>22</sup>

In these regards, Swartz’s situation is similar to that in *United States v. McCarthy*, 77 F.3d 522 (1<sup>st</sup> Cir. 1996). In *McCarthy*, the defendant left a suitcase unlocked and open in the back room of his landlord’s trailer, a room to which he did not have exclusive access, and in any

---

<sup>22</sup> See *Curlin*, 638 F.3d at 565; see also *United States v. McRae*, 156 F.3d 708, 711 (6th Cir. 1998) (holding that defendant had no legitimate expectation of privacy in a vacant house in which he had been living for a week); *United States v. Sanchez*, 635 F.2d 47, 64 (2d Cir. 1980) (refusing to suppress photographs taken from secret compartments in rear wheel wells of car parked outside defendant’s apartment building for a week and to which he possessed the keys, because car was registered to someone else and defendant could not demonstrate ownership or permission to possess the car) (citing *Rakas*); *Amezquita v. Hernandez-Colon*, 518 F.2d 8, 11 (1st Cir. 1975) (holding that squatters formerly evicted from public land had no expectation of privacy in homes they unlawfully constructed there); *United States v. Ruckman*, 806 F.2d 1471, 1472-74 (10th Cir. 1986) (holding that individual lacked expectation of privacy in contents of cave in which he resided as a trespasser on federal land); *United States v. Gale*, 136 F.3d 192, 195 (D.C. Cir. 1998) (holding that individual lacked legitimate expectation of privacy in apartment he occupied without permission of its tenant or other legal authority); *United States v. Rambo*, 789 F.2d 1289, 1295-95 (8th Cir. 1986) (holding that hotel occupant who was asked to leave by police officers acting on behalf of hotel management no longer had a reasonable expectation of privacy in hotel room).

event after he had been told to leave the trailer. *Id.* at 535. Police took the suitcase and inventoried it without a warrant. *Id.* at 528. The First Circuit upheld the search, noting that the defendant “clearly had assumed the risk that [his landlord] might consent to a search of the room (and that the search would extend to any items, like the suitcase, sitting open in plain view). Moreover, [the defendant]’s legitimate expectation argument is further undercut by the fact that he left the open suitcase in [the landlord]’s trailer after [the landlord] told [the defendant] that he and [another] had to leave.” *Id.* at 535 (citations omitted).

**B. MIT Consented to the Searches and Had the Right to Do So**

MIT consented to the search of its own closet and the closet’s contents, and MIT had the right to do so. *See, e.g., Schneckloth v. Bustamonte*, 412 U.S. 218, 222 (1973) (“A search conducted pursuant to a valid consent is constitutionally permissible.”); *U.S. v. Matlock*, 415 U.S. 164, 172 n.7 (1974) (a person with common authority over premises or effects can consent to search). Swartz assumed the risk that MIT would consent to the search when he attached the laptop to MIT’s network switch surreptitiously and left it hidden for extended periods. *Cf. McCarthy, supra* (upholding search of former tenant’s suitcase when invited by landlord).

**C. Officers Were Lawfully Inside The Wiring Closet and Student Center Office and Could Seize The Laptop and Hard Drive Without a Warrant Because They Were in Plain View**

Even if Swartz had a reasonable expectation of privacy in MIT’s wiring closet and its contents or the student center office and its contents, and even if MIT had not consented to the search of its closet and office, the computer and hard drive were lawfully seized, fingerprinted, and examined because they were in plain view where officers were lawfully present and the officers had probable cause to believe that they were evidence.

**1. *Officers Were Inside MIT's Wiring Closet Lawfully at MIT's Request***

Law enforcement officers were lawfully present in MIT's wiring closet. MIT consented to, and in fact solicited, law enforcement's presence and investigation. This is uncontested.

**2. *MIT Lawfully Showed Officers The Computer Equipment They Had Found Under the Cardboard Box***

The Fourth Amendment "is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (internal quotation marks omitted). As a result, the Fourth Amendment is not violated when private party acts on its own accord, conducts a search, and shares the results with law enforcement. *See id.* Similarly, agents who learn of evidence via a private search may reenact the original private search without violating any reasonable expectation of privacy. *See id.* *See also United States v. Miller*, 152 F.3d 813, 815-16 (8th Cir. 1998); *United States v. Donnes*, 947 F.2d 1430, 1434 (10th Cir. 1991).

Under these principles, MIT validly showed officers the computer equipment it had found beneath the box, and the officers lawfully recreated MIT's searches.

**3. *Officers May Seize Items in Plain View Upon Probable Cause to Believe that the Items are Evidence of a Crime***

Once officers encountered the laptop and the hard drive in plain view, they could seize the equipment lawfully without a warrant because they had probable cause to believe that it was evidence of a computer crime. *See United States v. Paneto*, 661 F.3d 709, 713 (1<sup>st</sup> Cir. 2011) ("One such exception [to the warrant requirement] is for items in plain view. A police officer, even though he does not have a search warrant, may seize an object in plain view as long as he

has lawfully reached the vantage point from which he sees the object, has probable cause to support his seizure of that object, and has a right of access to the object itself.”); *id.* at 714 (“In general terms, probable cause exists when police have sufficient reason to believe that they have come across evidence of a crime.”). “The seizure of property in plain view involves no invasion of privacy and is presumptively reasonable, assuming there is probable cause to associate it with criminal activity.” *Payton v. New York*, 445 U.S. 573, 587 (1980). *See also Texas v. Brown*, 460 U.S. 730 (1983) (same).

Swartz claims that his equipment was not in plain view in the wiring closet because he had hidden it under a cardboard box. There was no Fourth Amendment search when MIT employees looked under the box or when they showed police the equipment they had found there. *See supra*. But even if MIT employees had not already lifted the box to expose the computer equipment, an item in an opaque container can still be in plain view. “[S]ome containers (for example a kit of burglar tools or a gun case) by their very nature cannot support any reasonable expectation of privacy because their contents can be inferred from their outward appearance.” *Arkansas v. Sanders*, 442 U.S. 753, 765 (1979). There is no reasonable expectation of privacy in a container that discloses its contents. *United States v. Epps*, 613 F.3d 1093 (11th Cir. 2010) (no reasonable expectation of privacy in pillowcase with pink stains evidencing exploded dye pack following bank robbery). Here, the cardboard box disclosed its contents, because the officers knew that a hacker’s computer had been traced to that closet and they saw a wire running from the box to the network switch. Law enforcement officers immediately concluded that a hard drive was contained in the enclosure underneath the laptop because a USB cable went from the enclosure to the laptop and the enclosure was of a type used

to enclose external hard drives. Consequently, the cardboard box and the wire disclosed the box's contents and therefore the laptop and the hard drive were in plain view.

**4. *Officers May Manipulate and Search Items in Plain View Upon Probable Cause to Believe that the Items are Evidence of a Crime***

Because the equipment was in plain view and the officers had probable cause to believe that the equipment was evidence of a crime, the officers also could lawfully manipulate and search the equipment without a warrant by moving it around and opening it. "When an officer seeks to manipulate an object in plain sight, the relevant inquiry becomes whether the plain view doctrine would have sustained a seizure of the object itself." *Paneto*, 661 F.3d at 713-14 (upholding officer's picking up and examining \$20 bill in plain view in apartment because officer had probable cause to believe that it was the \$20 bill the officer had earlier given the defendant in a drug sting) (alterations and internal quotation marks omitted) (citing *Arizona v. Hicks*, 480 U.S. 321 (1987)).

Swartz counters the First Circuit's interpretation of *Arizona v. Hicks* in *Paneto* by contending that opening the laptop and attached hard drive case violated his Fourth Amendment rights. In *Hicks* a policeman was searching an apartment under exigent circumstances for a weapon. During the search, he noticed expensive stereo equipment. Suspecting (without probable cause) that the stereo equipment was stolen, he moved some of it to read and record its serial numbers. The Supreme Court held that although the officer was lawfully present in the apartment, moving the stereo equipment to identify its serial numbers was unlawful because this search was unsupported by probable cause. In other words, probable cause to look for a weapon does not necessarily give an officer probable cause to move stereo equipment without probable

cause to believe that the stereo equipment was evidence. However, while looking for a weapon, an officer *may* move stereo equipment if he has probable cause to believe that the stereo equipment is evidence. Indeed, the Court addressed this very point:

Justice Powell's dissent reasonably asked what it is we would have had Officer Nelson do in these circumstances. *The answer depends, of course, upon whether he had probable cause to conduct a search*, a question that was not preserved in this case. *If he had, then he should have done precisely what he did [i.e., moved the stereo equipment for further examination].*

*Hicks*, 480 U.S. at 329 (emphasis added).

In the present case, investigators had probable cause to believe that the computer and attached laptop were instrumentalities of a crime. They further had probable cause to believe that the equipment would bear fingerprints that would be evidence of the crime. Fingerprinting the equipment was fully consistent with *Hicks*. Indeed, as is apparent from the quotation, it would have been encouraged.

#### 5. *Swartz's Cases Concerning Searching the Contents of a Computer's Files Are Inopposite*

Swartz cites four cases in his brief for the proposition that "internal examination" of the laptop by the police constituted a Fourth Amendment search. *See* Def.'s Motion to Suppress No. 1 at 13-14. Swartz's cases are inopposite because they concern searches of computers' electronic files, not searches of a computers' exteriors and screens. The Government does not contend that a computer in plain view can necessarily have its files searched without a warrant.<sup>23</sup>

---

<sup>23</sup> Swartz argues that a network scan to determine which ports (network connection points) his computer had open was a search within the meaning of the Fourth Amendment. Def.'s Motion to Suppress No. 1 at 13-14. The ports used by a computer to communicate on a network are in electronic plain view, just as are the IP addresses used by the computer to



Indeed, the Government sought and obtained a warrant for this purpose.

It was also proper under the exigent circumstances described below.

**B. Exigent Circumstances Justified an Attempt to Copy the Laptop's RAM**

When MIT and the officers arrived at the wiring closet on January 4, 2011, they did not know who had connected the laptop to MIT's network, whether it was being used for any other illegal purposes in addition to the downloads, or how soon the hacker might return and take the laptop. After crime scene specialists had fumed the laptop for fingerprints, Special Agent Pickett sought, unsuccessfully, to copy the laptop's Random Access Memory ("RAM").<sup>24</sup> This was lawful. "Government agents may conduct a warrantless search or seizure if (1) probable cause supports the search or seizure and (2) 'exigent circumstance' exist. Exigent circumstances include imminent destruction of evidence, a threat to the safety of law enforcement officers or the general public, 'hot pursuit' of a suspect by police, or likelihood that suspect will flee before the officer can obtain a warrant." 41 Geo. L.J. Ann. Rev. Crim. Proc. 83 (footnote omitted, collecting cases). *See also Schmerber v. California*, 384 U.S. 757, 766-72 (1966) (exigent circumstances justified warrantless search of blood sample to test alcohol level because police had probable cause to arrest and feared destruction of the evidence by dissipation of alcohol in

---

communicate. *See supra* at 15-17. Nevertheless, the Government does not intend to offer this information in evidence in its case-in-chief and therefore this aspect of his motion is moot.

<sup>24</sup> Law enforcement officers are not uniformly clear as to whether the laptop's screen was showing a logon screen when they opened the laptop to fingerprint it or whether the logon screen appeared only when they attempted to copy the laptop's RAM. Regardless, officers legitimately opened the laptop's cover for the multiple reasons described above, putting the logon screen in plain view. If the logon screen did not appear until officers touched the laptop's keyboard, touching the keyboard was lawful under *Hicks* – there was probable cause to believe that the logon screen would show evidence of who owned the laptop.

the blood). “Exigent circumstances occur when a reasonable officer could believe that to delay acting to obtain a warrant would, in all likelihood, permanently frustrate an important police objective, such as to prevent the destruction of evidence relating to criminal activity . . . .”

*United States v. Rengifo*, 858 F.2d 800, 805 (1st Cir. 1988).<sup>25</sup>

Agent Pickett was reasonable in his belief that if officers delayed copying the RAM while they obtained a warrant, they might permanently lose access to significant evidence. A computer contains two types of information: information stored on the hard disk remains after the computer is turned off, whereas information stored in RAM is completely lost when the computer is turned off. Despite its volatility, RAM information can assist an investigation in several ways, including providing the computer’s decryption passwords. Without these passwords, the computer can for all intents and purposes be impossible to search later, despite having a valid search warrant. Accordingly, exigent circumstances justified Special Agent Pickett’s efforts to copy the laptop’s RAM without a warrant before the perpetrator could access his computer again and power it down.

To copy the RAM, officers needed to access the computer’s screen and keyboard. Viewing the laptop’s screen was merely incidental to the lawful exigent effort to copy the laptop’s RAM.

---

<sup>25</sup> In an analogous situation, courts have repeatedly upheld searching a cell phone’s call log incident to arrest on the grounds that incoming calls can cause the least recent calls to be erased. *See e.g., United States v. Valdez*, 2008 WL 360548 (E.D. Wis. 2008); *United States v. Mercado-Nava*, 486 F.Supp. 2d 1271, 1278 (D. Kan. 2007); *United States v. Parada*, 289 F. Supp. 2d 1291, 1303-04 (D. Kan. 2003).

**C. Discovery Was Inevitable After Officers Obtained Warrants to Search Seized Equipment**

Even had a warrant been necessary to search the laptop and hard drive on January 4th, the results of these searches would have been discovered inevitably after the officers obtained warrants to search them later on. “Although evidence derived from unlawful searches is generally subject to suppression, there are numerous exceptions to this rule. One such, the inevitable discovery exception, applies to any case in which the prosecution can show by a preponderance of the evidence that the government would have discovered the challenged evidence had the constitutional violation to which the defendant objects never occurred.” *United States v. Scott*, 270 F.3d 30, 42 (1st Cir. 2001) (citing *Wong Sun v. United States*, 371 U.S. 471, 484-87 (1963) and *Nix v. Williams*, 467 U.S. 431, 440-48 (1984)). The inevitable discovery rule has three factors:

[A]re the legal means truly independent; are both the use of the legal means and the discovery by the means truly inevitable; and does the application of the inevitable discovery exception either provide incentive for police misconduct or significantly weaken Fourth Amendment protection?

*United States v. D’Andrea*, 648 F.3d 1, 12 (1st Cir. 2011) (quoting *United States v. Silvestri*, 787 F.2d 736, 744 (1st Cir. 1986)).

The Government obtained warrants to search the laptop and hard drive on February 24<sup>th</sup>, evincing its intention that the two would inevitably be searched. The warrants were independent of the January 4th searches: their affidavits did not rely upon or even refer to the fingerprints, what was seen on the laptop screen, or the contents of the packet capture. Finally, there was no police misconduct (intentional or unintentional) that would be encouraged by applying the inevitable discovery doctrine.

Accordingly, if the Court determines that any evidence recovered on January 4th was recovered unlawfully, the Court should nonetheless find it admissible because it would inevitably have been discovered when the independently obtained lawful warrants were subsequently executed.

**V. MOTION TO SUPPRESS FRUITS OF UNLAWFUL ARREST AND SEARCH OF HP USB DRIVE (No. 3)**

Swartz next moves to suppress the USB drive recovered incident to his arrest and subsequently searched pursuant to a warrant. His USB drive contains a version of the software that Swartz used to download JSTOR's articles. This motion must be denied because there was probable cause both to arrest Swartz on January 6, 2011, and to search the USB drive recovered from his backpack incident to his arrest.

**A. Probable Cause to Arrest Aaron Swartz on January 6, 2011**

***1. Facts Known at the Time of Arrest***

When MIT Police Captain Albert Pierce and others arrested Swartz on January 6, 2011, there were facts sufficient to establish probable cause that Swartz had committed several crimes. At a minimum, arresting officers knew, as reflected in the report attached to the initial charging complaint (Ex. 19):

- (1) A person had entered a restricted telephone and networking closet whose access was controlled by MIT;
- (2) That person had connected a laptop and external hard drive directly to a networking switch without authorization;
- (3) That person had hidden the equipment under a cardboard box;
- (4) The laptop had illegally downloaded scientific periodicals from JSTOR;
- (5) The person had downloaded gigabytes of data from JSTOR, valued in the

tens of thousands of dollars at the time;

- (6) The suspect he was about to interview looked just like the person who had just been seen on a video removing the equipment from the closet;
- (7) The suspect was near MIT, the scene of the crime; and
- (8) The suspect he was about to interview fled when approached by police.

**2. *Probable Cause to Arrest for Federal and State Computer Crime Violations, Among Others***

On these facts, officers had objective probable cause to believe that Swartz had accessed MIT's computer system without authorization and thereby taken substantial amounts of data from JSTOR. Thus, at the time of arrest, they had objective probable cause to believe that Swartz had violated at least two computer crime statutes: Massachusetts General Laws ch. 266, § 120F and 18 U.S.C. § 1030(a)(2)(C). There was probable cause to believe that Swartz had violated the state computer crime statute, because it punishes "[w]hoever, without authorization, knowingly accesses a computer system by any means, or after gaining access to a computer system by any means knows that such access is not authorized and fails to terminate such access," Mass. Gen. Laws ch. 266, § 120F. There was probable cause to believe that Swartz had violated the federal computer crime statute, because it similarly punishes whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains — (C) information from any protected computer," 18 U.S.C. § 1030(a)(2)(C). Swartz has not challenged, nor can he, the existence of probable cause to believe at the time of his arrest that he had committed state and federal computer crimes. Since officers had objective probable cause to arrest Swartz, the search instant to his arrest that recovered the USB drive from his backpack was also lawful.

Moreover, in addition to the computer crime statutes, the facts listed above also gave objective probable cause to believe that Swartz had violated all the other statutes on which he was later indicted: breaking and entering in the daytime with intent to commit a felony in violation of Massachusetts General Law ch. 266, § 18; larceny over \$250 in violation of Massachusetts General Laws ch. 266, § 30; wire fraud in violation of 18 U.S.C. § 1343; computer fraud in violation of 18 U.S.C. § 1030(a)(4); and reckless damage to a protected computer in violation of 18 U.S.C. § 1030(a)(5).

### **3. *The Officers' Subjective Assessment of Probable Cause is Irrelevant***

Swartz says that the officers lacked probable cause to arrest him for the state breaking and entering statute because the statute did not cover his conduct and they did not identify any other applicable criminal statutes at the time.

But the officers' *subjective* intent at the time of an arrest is irrelevant. An arrest and a search incident thereto are valid if the arresting officer had objective grounds for probable cause to arrest the defendant, even if the officer subjectively mistook which statute applied. *E.g.*, *Devenpeck v Alford*, 543 U.S. 146, 153-54 (2004) (holding that the “[s]ubjective intent of the arresting officer . . . is simply no basis for invalidating an arrest. Those are lawfully arrested whom the facts known to the arresting officers give probable cause to arrest.”); *United States v. Bookhardt*, 277 F.3d 558, 565 n.10 (D.C. Cir. 2010) (holding that existence of probable cause to arrest must be determined objectively from facts and circumstances known to officers at time of arrest without regard to subjective intentions of officers involved).<sup>26</sup> The officers' subjective

---

<sup>26</sup> See, similarly, *Barna v. City of Perth Amboy*, 42 F.3d 809, 819 (3d Cir. 1994) (holding that “[p]robable cause need only exist as to any offense that could be charged under the circumstances”); *United States v. Kalter*, 5 F.3d 1166, 1168 (8<sup>th</sup> Cir. 1993) (upholding arrest

intent is irrelevant even if they mistakenly charged a defendant with a state crime but had objective probable cause to believe that the defendant had committed a federal crime. *See United States v. Pollack*, 739 F.2d 187, 199 (5<sup>th</sup> Cir. 1984) (“If, as in the instant case, the arresting officer knows facts which constitute probable cause to believe that the suspect has committed a federal crime, it is not required that the officers subjectively believe that probable cause exists to arrest for that crime. Thus [the agent’s] mistaken belief regarding a \$5,000 [federal] jurisdictional requirement is not fatal.”).

Consequently, the Court should focus on the fact that the officers had objective probable cause to arrest Swartz on the various statutes listed above and should ignore the officers’ identification of different statutes at the time of arrest.

**4. *Officers Nonetheless Had Probable Cause to Arrest Swartz for Breaking and Entering with Intent to Commit a Larceny***

Even were the arresting officers’ subjective intent relevant, the officers had probable cause to arrest Swartz for breaking and entering in the daytime with intent to commit larceny.

Swartz claims that he could not have committed this offense because he believed he had permission to be in the wiring closet. Whether Swartz believed that he had MIT’s permission to be in the closet is beside the point, because the *officers* had probable cause to believe that Swartz

---

because, although the police lacked probable cause to arrest defendant for concealed-weapon violation that was actual reason for the arrest, police nevertheless had probable cause to arrest him for violating a separate ordinance requiring that a gun be carried in a locked container); *United States v. Atkinson*, 450 F.2d 835, 838 (5<sup>th</sup> Cir. 1971) (declining to decide whether an arrest for false pretenses was legal because the officer had probable cause to arrest the defendant for operating a vehicle with an invalid license tag); *Kingler v. United States*, 409 F.2d 299, 303-06 (8<sup>th</sup> Cir. 1969) (upholding arrest because, although the police lacked probable cause to arrest the defendant for vagrancy, the charged offense, they had probable cause to believe that he had committed robbery); *see also* Wayne R. LaFave, *Search and Seizure* § 1.4(d) (3d ed. 1996) (collecting cases).

lacked permission and knew that he lacked permission.

Swartz also argues that he could not have committed a larceny because he did not “intend to deprive JSTOR of its property permanently, nor did the downloading have that effect.”

Swartz misinterprets the larceny statute. Massachusetts General Law chapter 266, § 30 was specifically amended in 1983 to include electronically processed or stored data to ensure that prosecutors could use it to prosecute the then-nascent problem of computer crime. Subsection 2 of the law now states, in pertinent part, that “‘Property’, as used in [section 30], shall include . . . electronically processed or stored data, either tangible or intangible, data in transit [and] telecommunications services.” Mass. Gen. Laws ch. 226, §30 (2). As stated by Representative Kenneth Lemanski in a letter to the governor’s legislative office (Ex. 20):

The most important aspect of this bill, in my opinion, is the fact that it now allows electronic impulses to be defined as property. This is essential to combating computer crime. . . [Prosecutors] will now be able to refer to a specific statute in the prosecution of what was formerly one of the most difficult types of crime. H.6227 directly attacks what, up until now, had been the judicial sticking point: are electronic data “property”? Our own Supreme Judicial Court agreed with earlier Federal Opinions that the answer was no, under the existing statutes. H.6227 remedies this by explicitly including computer data in the definition of property.

Thus understood, the statute does not exclude from coverage a hacker who copies his victim’s data. Nor should this Court make such a novel interpretation of Massachusetts law. “A statute should be constructed [to give effect] to all of its provisions, so that no part will be inoperative or superfluous, void or insignificant.” *Corley v. U.S.*, 556 US 303, 304 (2009). “It is an elementary rule of construction that effect must given, if possible, to every word, cause and sentence of a statute.” 2A *Sutherland Statutory Construction* § 46.06 (7<sup>th</sup> ed. 2007). All computer data theft involves copying. If the statute were interpreted to punish the data thief only if he erased the



victim's data, that would render the computer crime amendment largely inoperative.

In sum, at the time of arrest, there was objective probable cause to believe that Swartz had violated the state and federal computer crime statutes, plus several other state and federal statutes, including breaking and entering to commit larceny. The arrest and the seizure of the USB drive incident to arrest were therefore lawful.

### **B. Probable Cause to Search the USB Drive**

After the USB storage drive was seized incident to Swartz's arrest, the Government obtained a warrant to search the drive for violations of 18 U.S.C. § 1030(2)(2) (data theft); 18 U.S.C. § 1030(a)(5)(A) (intentional damage to a computer system) and 18 U.S.C. § 1343 (wire fraud). The Government then searched the drive pursuant to that warrant.

Swartz incorrectly contends that officers lacked probable cause to believe that the USB drive contained evidence of Swartz's crimes. A magistrate's decision to issue a warrant must be reviewed with great deference. A reviewing court should give significant deference to the magistrate judge's initial evaluation of an affidavit for a search warrant, reversing the magistrate judge only when there is no "substantial basis" for concluding that probable cause existed. *United States v. Ribeiro*, 397 F.3d 43, 48 (1st Cir. 2005) (citing *United States v. Feliz*, 182 F.3d 82, 86 (1st Cir. 1999)).

Moreover, Magistrate Judge Dein's conclusion that officers had probable cause to believe that the USB drive contained evidence was amply supported by the affidavit. As set forth in the affidavit (Ex. 21), Swartz had been videotaped entering the wiring closet on January 4, 2011, and again on January 6, 2011, shortly before he was arrested. (Aff. ¶¶ 22, 24.) He was arrested near MIT, the scene of the crime, shortly after the "ghost laptop" had been relocated to MIT's

Building W20. (Aff. ¶ 25). The crime involved using a program to download a large amount of information. (Aff. ¶¶ 12-19.) USB drives are frequently used to store software, data and records, including the type of records that were illegally downloaded from JSTOR. (Aff. ¶ 26). USB drives are also frequently used to transfer records and data between computers and hard drives, and Swartz had used two laptops on October 9, 2010. (Aff. ¶¶ 17, 18, 26). Because Swartz was arrested on the afternoon of the day he was last seen in the wiring closet, there was reason to believe that he had the USB drive with him as he committed the crime.

Probable cause does not require a certainty of finding evidence. All that is needed is a “reasonable likelihood” that incriminating evidence will turn up during a proposed search. *United States v. Clark*, 685, F3d. 72, 76 (1st Cir. 2012). The facts set forth above established a more than reasonable likelihood that the USB drive would hold records relevant to the crime.

Even assuming that Agent Pickett’s search warrant affidavit was lacking, the evidence seized pursuant to the warrant should nonetheless be admitted under the good-faith doctrine enunciated in *United States v. Leon*, 468 U.S. 897, 922 (1984). In *Leon*, the Supreme Court held that evidence seized in good-faith reliance on a warrant later found defective is admissible at trial. *Id.* There are four exceptions in which the good-faith exception may not be invoked: (1) when the magistrate was misled by false information that the affiant knew was false or should have known was false but for his reckless disregard for the truth; (2) when the magistrate wholly abandoned her neutral role; (3) when the affidavit is so lacking in indicia of probable cause that no reasonable officer could believe to the contrary; and (4) when a warrant is so facially invalid, as by failing to describe with particularity the premises to be searched, that no reasonable officer could believe it valid. *Id.* at 923; *see also United States v. Owens*, 167 F.3d 739, 745 (1st Cir.

1999). Here, none of those exceptions is present, and thus, even assuming *arguendo* that the search warrant affidavit was deficient, the Court should rule the evidence derived from the warrant is admissible.

**VI. MOTION TO SUPPRESS RESULTS OF SEARCHES OF SWARTZ'S APARTMENT AND OFFICE (No. 4)**

Swartz's fourth motion to seeks to suppress the results of the searches of his apartment and his office, even though those searches were performed subject to search warrants. Because the Government will not introduce any evidence from the searches during its case in chief, nor evidence derived from those searches, this motion is moot.

The Government reserves the right to cross-examine Swartz about his statements and actions during and after those searches if he testifies on his own behalf.<sup>27</sup>

**VII. MOTION TO SUPPRESS FRUITS OF SEARCHES OF SEIZED COMPUTER EQUIPMENT (No. 5)**

Swartz's final motion seeks to suppress the searches of the laptop and the hard drive that were seized on MIT's property and the USB drive that was seized from Swartz incident to his arrest, all of which were searched pursuant to federal search warrants. Swartz seeks suppression because, he contends, the Government should have obtained and executed the warrants sooner, and thereby the Government unlawfully interfered with his possession of his equipment.

The motion should be denied. Having left the equipment unattended for months at MIT, having had it properly seized as physical evidence by the police under exceptions to the Fourth

---

<sup>27</sup> Even were the defendant's statements derivative of a Fourth Amendment violation — which they were not — they would be admissible for impeachment purposes. *See e.g., U.S. v. Torres*, 926 F.2d 321, 323 (3rd Cir. 1991) (evidence obtained in violation of Fourth Amendment admissible to impeach defendant's testimony).

Amendment's warrant requirement, and having not sought the equipment's return before the warrants' issue, any rights that Swartz might theoretically have had to the equipment's return were not meaningfully infringed while the Cambridge Police Department held the evidence in their case and the Secret Service sought warrants to search them for their federal investigation.

**A. *Swartz Claims that the Police Improperly Held the Equipment After He Was Arrested and Charged***

Swartz asserts an unusual basis for relief in his fifth motion to suppress. He does not argue here that the equipment was seized improperly or that the warrants failed to articulate probable cause to believe that the equipment contained evidence of a crime.<sup>28</sup> Rather, he argues solely that the officers' delay in obtaining the warrants unreasonably interfered with his possessory interests. *See* Def.'s Motion to Suppress (No. 5) at 3 (“[E]ven a seizure lawful at its inception can nevertheless violate the Fourth Amendment because its manner of execution infringes *possessory interests* protected by the Fourth amendment’s prohibition on “unreasonable searches.””) (quoting *United States v. Jacobson*, 466 U.S. 110, 124 (1984)) (emphasis added). *See also United States v. Burgard*, 675 F.3d 1029, 1033 (7<sup>th</sup> Cir. 2012) (“On the individual person’s side of this balance [of reasonableness], the critical question relates to any possessory interest in the seized object, not to privacy or liberty interests. A seizure affects only the person’s possessory interests; a search affects a person’s privacy interests.”) (internal quotation marks and citations omitted), *cert. denied*, 2012 WL 2002441 (Oct. 1, 2012).

In other words, this motion focuses not on what the officers found inside the equipment, or even how they found it, but rather on the Cambridge Police Department’s retention of the

---

<sup>28</sup> To the extent that the motion does raise these arguments, the Government disposed of them when responding to Swartz’s earlier motions to suppress.

equipment in a pending state criminal case before the Secret Service obtained and executed warrants in the federal investigation.

***B. The Cambridge Police Properly Seized and Held the Laptop, Hard Drive and USB Drive as Physical Evidence***

The Cambridge Police Department properly seized and held the laptop, the hard drive, and the USB drive as *physical evidence* in their state case under exceptions to the Fourth Amendment's warrant requirement. The equipment constituted physical evidence of computer crimes, larceny, and breaking and entering, just as a bag of burglar tools or a bag of stolen goods would be physical evidence if recovered at the scene of a crime or if seized incident to a burglar's arrest. *See supra*. The police accordingly had an objective basis to deprive Swartz of possession of the equipment throughout the period they held it in their evidence locker, a basis that was wholly independent of the Secret Service's subsequent searches of the equipment's contents.

Swartz does not contend – nor could he credibly contend – that the Cambridge police had an insufficient basis for continuing to hold the laptop and hard drive as physical evidence pending trial, even if the Secret Service had never obtained warrants to examine their contents. The laptop and the hard drive were in the closet to which the unauthorized downloads had been traced. A physical wire extended from the laptop and hard drive to MIT's network, and a virtual wire connected MIT's network to JSTOR's database. The laptop could be used to conduct the unauthorized downloads — the burglar's tools — and both the laptop and the hard drive could be used to store the articles — the loot. In this sense, they were the last physical links in the theft of JSTOR's articles. And they were instrumentalities of a crime which need not have been returned to the suspected perpetrator.

While one step removed, the Cambridge police had a sufficient basis to continue to hold the USB drive seized from Swartz incident to his arrest as physical evidence, as well. Swartz was arrested near MIT, within hours of having last been seen in the wiring closet. His crime involved the use of a program to download a large amount of information. USB drives are frequently used to store software applications, data and records, including the type of records that were illegally downloaded from JSTOR. They are also frequently used to transfer records and data between computers and hard drives, and MIT's records indicated that the perpetrator had used two laptops when executing his crime on October 9, 2010. *See supra*.

When an officer lawfully seizes property without a warrant because of probable cause to believe that it constitutes evidence of a crime, the officer may hold on to that evidence without a warrant and therefore the defendant has no grounds to complain that the officers delayed in searching it. *See United States v. Carter*, 139 F.3d 424, 426 (4th Cir. 1998) (en banc) (denying motion to suppress because of excessive delay between seizure of suitcase incident to arrest and issuance of search warrant, because the suitcase itself was evidence of the crime apart from the suitcase's contents); *United States v. Wright*, 2010 WL 841307 at \*8-\*10 (E.D. Tenn. Mar. 3, 2010) (holding almost month-long delay between seizure of laptop computer and application for warrant not unreasonable, because the laptop had evidentiary value in and of itself, apart from its contents, since the suspect's pre-arrest communications made it probable that the suspect would arrive at a destination with a computer); *id.* at \*9 ("And as *Mitchell* itself indicates, the Government is under no obligation to return property if it has 'some other evidentiary value.'") (quoting *United States v. Mitchell*, 565 F.3d 1347, 1352 (11th Cir. 2009)). Cases that Swartz cites for the contrary position are typically factually inapposite in one of two critical respects:

either the court never considered whether the searched computer or cellphone was physical evidence of a crime independent of its contents, or the court rejected the argument that the equipment was physical evidence of the crime.<sup>29</sup> Others are even less germane narcotics cases.<sup>30</sup> In sum, there was no infringement of Swartz's possessory interests in the computer equipment before it was searched pursuant to federal warrants, because it was being lawfully held during this time as physical evidence and instrumentalities of criminal activity.

***C. Swartz Never Asked for Any of the Equipment Back During the Period He Now Claims His Possessory Interests Were Wrongfully Infringed Upon***

At no time before the warrants were issued did Swartz or his counsel seek the return of

---

<sup>29</sup> See *United States v. Burgard*, 675 F.3d 1029 (7th Cir. 2012) (cellphone seized on probable cause to believe that the phone would contain evidence of a crime; no argument that the phone was evidence of a crime apart from its contents); *United States v. Mitchell*, 565 F.3d 1347, 1352 (11th Cir. 2009) (noting that the government would not have been obligated to return the computer if it had evidentiary value apart from its contents; no argument for that the computer was evidence apart from its contents); *United States v. Rubinstein*, 2010 WL 2723186 at \*12-\*14 (S.D. Fla. June 24, 2010) (no argument computer seized at the border was evidence independent from the files it contained); *United States v. Riccio*, 2011 WL 4434855 (S.D. Cal. Sept. 23, 2011) (no argument that phone was evidence apart from its contents); *United States v. Shaw*, 2012 WL 844075 at \*3 (N.D. Ga. May 25, 2012), (evidentiary value of cellphones seized incident to an arrest in a drug conspiracy was not readily apparent without regard to the information to be found in the telephones).

One case cited by Swartz, *United States v. Budd*, 549 F.3d 1140, 1147-48 (7<sup>th</sup> Cir. 2008), actually helps the Government because it holds that even if officers waited too long in obtaining a warrant to seize a computer, the search of the computer pursuant to the warrant would not be suppressed under the independent source doctrine if the affidavit was premised on information that had not been obtained from the computer during its illegal detention.

<sup>30</sup> See *United States v. Jacobson*, 466 U.S. 109, 122, 124-25 (1984) (affirming that officer may seize property without a warrant based on probable cause to believe that it contains contraband and that officers did not need a warrant to destroy a small amount of suspected cocaine to perform a field test); *Segura v. United States*, 468 U.S. 796 (1984) (holding that officers who had probable cause to believe an apartment contained a criminal drug operation but entered illegally, nevertheless did not violate the Fourth Amendment by securing the apartment through the night and into the next day while obtaining a warrant to search the apartment).

the laptop, the hard drive, or the USB drive: not by formal motion in state or federal court and not by informal request of either the state or federal prosecutors. Indeed, Swartz did not even ask for a copy of the files stored on the equipment until the formal discovery process began much later in the state and federal court cases.

Where a property-owner fails to demand that officers return his equipment before they obtain a warrant, he cannot later argue that his possessory interests were harmed by a delay in obtaining a warrant. If Swartz needed the equipment back, he should have asked for its return at the time. *See United States v. Stabile*, 633 F.3d 219, 235-36 (3d Cir. 2011), *cert. denied*, 132 S. Ct. 399 (2011) (holding that three-month delay between seizure and obtaining a warrant to search hard drives not unreasonable, based in significant part on the grounds that a defendant who does not request the return of his property cannot argue that pre-warrant delay adversely affected his Fourth Amendment rights) (citing *United States v. Johns*, 469 U.S. 478, 487 (1985)); *United States v. Ivers*, 430 Fed. App'x 573, 576, 2011 WL 1594652 at \*2 (9<sup>th</sup> Cir. April 28, 2011) (rejecting defendant's argument that the FBI violated Fed. R. Crim. P. 41 by taking more than 10 days to execute a search warrant, because "[t]o the extent that the government unlawfully deprived Ivers of his property, Ivers was not without recourse. He could have filed a motion to return property at any time. Fed. R. Crim. P. 41(g). He simply did not do so."); *Unites States v. Lowe*, 2011 WL 1831593 at \*3 (S.D. Tex. May 12, 2011) (distinguishing *Mitchell* in part on the ground that the defendant never asked for the return of the searched property before the search warrant was obtained and there was "therefore no reason to believe that the defendant's possessory interests in the cell phone were substantially interfered with."). Because Swartz did not ask the Government to return his equipment before the warrants issued,



under *Johns*, *Stabile*, *Ivers*, and *Lowe*, his motion to suppress for pre-warrant delay must be denied.

***D. Swartz's Possessory Interests in the Laptop and Hard Drive Were Attenuated Because He Left Them Unattended for Extended Periods on MIT Property and Didn't Request Their Return***

In the alternative, any delay in obtaining the warrants to search the laptop, hard drive and USB drive had no cognizable effect on Swartz's possessory interests, because those interests were highly attenuated even before the equipment was seized. After officers seize property, there is no strict time limit within which they must obtain a warrant to search it. Whether pre-warrant delay is unreasonable is decided case by case. "There is unfortunately no bright line past which a delay becomes unreasonable. Instead, the Supreme Court has dictated that courts must assess the reasonableness of a seizure by weighing the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion." *Burgard*, 675 F.3d at 1033 (internal quotation marks and citations omitted).

In balancing the individual's interests in his property against the government's interests in an investigation, the Court must consider the nature of the individual's possessory interests. If the individual gave others access to that property, or left that property in others' hands, then his possessory interests are attenuated and a pre-warrant delay affects those interests much less. *See United States v. Martin*, 157 F.3d 46, 54 (2d Cir. 1998) (holding delay not unreasonable because, in part, "seizure is necessarily less intrusive where the owner has relinquished control of the property to a third party as was the case here [stolen equipment sold to third-party and then returned to defendant via commercial carrier, from which the equipment was seized]," and

seizing the property would not effectively restrain the liberty interests of the person from whom the property was seized, as with the seizure of a traveler's luggage); *see also United States v. Vallimont*, 378 Fed. App'x 972, 2010 WL 1857361 at \*3-\*4 (11<sup>th</sup> Cir. May 11, 2010), *rehearing and rehearing en banc denied*, 408 Fed. App'x 346 (11<sup>th</sup> Cir. 2010) (table) (distinguishing *United States v. Mitchell*, 565 F.3d 1347 (11<sup>th</sup> Cir. 2009), to find that a 45-day delay was not unreasonable in part because the defendant had a diminished privacy interest in his computer after having revealed its contents to a third party who could freely access its contents).

For the better part of three months before the seizure of the laptop and hard drive in Building W20, Swartz had only a tenuous possessory interest in the tools of his electronic theft. Swartz left his laptop and a series of five hard drives for extended periods at a time (1) running a high-speed downloading program unattended, (2) on MIT's property, (3) from which they would likely be removed by MIT personnel if discovered, (4) under circumstances intended to conceal that the equipment belonged to him and consequently would prevent its return to him. Even when Swartz retrieved the equipment on January 6, he again left it at another MIT building and room accessible to third parties. The slender possessory interests Swartz did have in the equipment were further thinned when he never even asked to have it returned to him before the search warrants were issued. *See supra*. The minimal possessory interests Swartz had in the equipment under the circumstances were outweighed by the government's interests in investigation.

***E. The Secret Service, Which Obtained the Warrant, Was Not the Same Entity that Seized the Equipment***

In yet another aspect, Swartz's assertion that the Secret Service infringed his possessory interests by delaying in obtaining a search warrant does not quite fit this situation or his legal

theory. The Secret Service did not seize his laptop, hard drive, or USB drive on January 6, 2011: the Cambridge Police Department did. Nor did the Secret Service possess this equipment before obtaining the warrants: the Cambridge Police Department did. Thus, the United States did not affect Swartz's possessory interests in his equipment until it executed warrants.

For all the reasons given above, the Cambridge Police Department did not seize or hold onto the equipment impermissibly long. The Cambridge Police Department was supporting a valid investigation and prosecution by the Commonwealth. But if the Court disagrees, then Swartz cannot simply morph allegations that local police held evidence too long in a local prosecution into a claim that federal law enforcement officers did so in a subsequent federal case.

#### ***F. The Delay Was Justified***

Finally, regardless of whether the interference with Swartz's possession was pegged to the Cambridge Police Department or to the Secret Service, the investigators had reason for the delay. Lengthy pre-warrant delays can be reasonable if the officers' other duties interceded and the officers took their duties on the present case seriously. *See Vallimont*, 378 Fed. App'x at 976 ("For example, a delay could be justified if the assistance of another law enforcement officer had been sought, or if some overriding circumstances arose, necessitating the diversion of law enforcement personnel to another case.") (internal quotation marks omitted) (citing *United States v. Mitchell*, 565 F.3d 1347, 1352-53 (11<sup>th</sup> Cir. 2009)); *see also Stabile*, 633 F.3d at 236 (allowing delay in part because of agent's unavailability).

Here, the police and federal investigators were called in to investigate a complex computer crime on January 4, 2011. Through good fortune, they identified the suspect on

January 6, 2011. They still needed, however, to investigate what Swartz did and how he did it. That involved identifying and debriefing witnesses, obtaining technical and specialized information from both MIT and JSTOR, consulting with experts, and learning the facts both to understand the facts well and how to explain them with clarity and accuracy in warrant applications. Given that some of the equipment had been in MIT's hands for months beforehand, that Swartz did not ask for its return, and that the officers already had probable cause to hold onto the pieces of equipment as physical evidence in and of themselves without regard for their contents, any pre-warrant delay was reasonable. Although the officers theoretically might have obtained a warrant more quickly, "police imperfection is not enough to warrant reversal [for delay in obtaining a warrant]. With the benefit of hindsight, courts 'can almost always imagine some alternative means by which the objectives of the police might have been accomplished,' but that does not necessarily mean that the police conduct was unreasonable." *Burgard*, 675 F.3d at 1034 (quoting *United States v. Sharpe*, 470 U.S. 675, 686-87 (1985)) (finding police's delay in obtaining a warrant not unreasonable because although the police might have been able to work more quickly, he did not completely abdicate work or fail to see the urgency of the task).

Here, the officers were sufficiently diligent.

## VII. CONCLUSION

For the reasons given above, the Court should deny all of Swartz's motions to suppress evidence.

Respectfully submitted,

Carmen M. Ortiz  
United States Attorney

By: /s/ Scott L. Garland  
STEPHEN P. HEYMANN  
SCOTT L. GARLAND  
Assistant U.S. Attorneys

### CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing.

/s/ Scott L. Garland  
SCOTT L. GARLAND  
Assistant United States Attorney

Date: November 16, 2012

Upon clicking the PDF link to obtain the article, the user is prompted with the Terms & Conditions overlay and must click Proceed to PDF in order to begin the download (note: this is a one time click through per session)

JSTOR: Search Results

www.jstor.org/action/doBasicSearch?Query=kittens&acc=on&wc=on

Hinchy ITHAKA Larsen

JSTOR HOME SEARCH BROWSE MyJSTOR

Search

Search Results

kittens

SEARCH

☐ Search within these results

SHOWING 1-25 OF 4312

Sort by Relevance GO Display 25 per page GO

MODIFY SEARCH

Show:

All results | Only results with images

All content | Only content I can access

Save Citation Email Citation Export Citation Track Citation

☐ Select/unselect all

1. Cortical Plasticity in Monocularly Deprived Immobilized Kittens Depends on Eye Movement  
R. D. Freeman, A. B. Bonds  
Science, New Series, Vol. 206, No. 4422 (Nov. 30, 1979), pp. 1093-1095  
PDF Summary

2. Fatal J. P. D. The J. PDF

3. Deple Taku. Stolen PDF

4. Exposure of Kittens and Puppies to Single Metacercariae of Paragonimus wesjermani from Taiwan  
P. C. Fan, C. H. Chiang  
The Journal of Parasitology, Vol. 56, No. 1 (Feb., 1970), pp. 48-54  
PDF Summary

5. Suckling Behaviour in Kittens  
R. F. Ewer  
Behaviour, Vol. 15, No. 1/2 (1959), pp. 146-162  
PDF Summary

6. Attempts to Assay the Enterotoxigenic Substance Produced by Staphylococci by Parenteral Injection of Monkeys and Kittens  
Ellen Davison, G. M. Dack, W. E. Cary  
The Journal of Infectious Diseases, Vol. 62, No. 2 (Mar. - Apr., 1938), pp. 219-223  
PDF Summary

7. Maternal Influence in Learning by Observation in Kittens  
Phyllis Chesler

JSTOR Terms and Conditions

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions. JSTOR's Terms and Conditions provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Proceed to PDF

Legend:

- ✓ You have access to this content
- ✓ You have access to part of this content
- ✗ Full text on external site
- ★ Citation access — see access options

Your access to JSTOR provided by JSTOR

SAVE THIS SEARCH

Search Name

Alert Me About New Articles

Weekly

SAVE RSS feed



---

Review: [untitled]  
Author(s): Jacqueline Long  
Source: *Classical Philology*, Vol. 86, No. 4 (Oct., 1991), pp. 357-364  
Published by: [The University of Chicago Press](#)  
Stable URL: <http://www.jstor.org/stable/270097>  
Accessed: 09/ 10/ 2010 12:41

---

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/page/info/about/policies/terms.jsp>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/action/showPublisher?publisherCode=ucpress>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.



*The University of Chicago Press* is collaborating with JSTOR to digitize, preserve and extend access to *Classical Philology*.

<http://www.jstor.org>

## The JSTOR Platform Terms and Conditions of Use

The JSTOR Platform is a trusted digital repository providing for long-term preservation and access to leading academic journals and other scholarly materials from around the world. JSTOR is part of ITHAKA, a not-for-profit organization with a mission to help the scholarly community take advantage of advances in technology, and is supported by libraries, scholarly societies, publishers, and foundations.

These Terms and Conditions of Use apply to individuals and institutions accessing content through JSTOR and, where applicable, are subject to the agreement entered into between JSTOR and a user's affiliated institution, such as a user's college or university. If you have questions about your affiliated institution's participation agreement with JSTOR, please contact your librarian.

Please note that these Terms and Conditions of Use may vary depending on the Collection or Content you are accessing and/or whether your institution is subject to grant-related project terms. *Please see Section 12 of these Terms and Conditions of Use for additional information.*

### 1. Definitions:

"Authorized Users" means

- (a) individuals who are affiliated with an Institutional Licensee, as defined below. This includes
  - (i) for educational non-profit and for-profit Institutional Licensees (such as colleges, universities, and secondary schools): currently enrolled students (including distance education students); on an ad hoc basis, researchers affiliated and/or visiting under the terms of an agreement with the Institutional Licensee; full and part-time staff; and on-site users physically present on the Institutional Licensee's premises ("Walk-In Users");
  - (ii) for museums; foundations; government agencies; corporate and for-profit organizations (other than for-profit educational organizations); and research center Institutional Licensees: full and part-time staff; on an ad hoc basis, researchers and lecturers affiliated and/or visiting under the terms of an agreement with the Institutional Licensee; and Walk-In Users;
  - (iii) for public library Institutional Licensees: full and part-time staff; Walk-In Users; and off-site users accessing the Licensed Content through a sessions-based arrangement entered into between JSTOR and the library;
- (b) individual members of scholarly societies that have entered into an agreement with JSTOR for access to specific Content via the JSTOR Platform ("Individual Access"); and
- (c) other users of specified content agreed upon in writing by or on behalf of JSTOR, including users of (i) Data for Research; (ii) the Publisher Sales Service (a service through which JSTOR facilitates users purchase of articles from publishers); and (iii) individual researchers not affiliated with a JSTOR participating institution, publication, or scholarly society.

"Content" means journal Back Issues and Current Issues, as defined in Sections 10.1 and 10.2, below, as well as portions of such journals, including articles and book reviews (each independently "Textual Content"); manuscripts and monographs (each independently also "Textual Content"); Data for Research (defined below); spatial/geographic information systems ("GIS") data; plant specimens ("Specimens"); and other materials made available by JSTOR.



“Data for Research” means data provided specifically for the purpose of textual extractions; describing and/or identifying content, usage, and operations; or cataloging information pertaining to the Content, to be used in research involving computational analysis rather than for purposes of understanding the intellectual meaning of such data.

“Institutional Licensee(s)” mean institution(s) that maintain(s) a valid Institutional Participation Agreement with JSTOR, available at <http://www.jstor.org/page/info/participate/new/forms.jsp>.

“JSTOR Platform” means JSTOR’s integrated digital platform, which delivers and preserves Content and is aimed at furthering access to scholarly materials by the worldwide scholarly community.

“Licensed Content” means the Content for which an Authorized User’s affiliated Institutional Licensee has entered into an Institutional Participation Agreement or other license agreement, or the Content available to an Authorized User through Individual Access, the Publisher Sales Service, or other programs. For more information about the JSTOR material licensed by your affiliated Institutional Licensee, please contact your librarian.

## 2. Use of the JSTOR Platform

2.1 Permitted Uses. Institutional Licensees and/or Authorized Users may search, view, reproduce, display, download, print, perform, and distribute Licensed Content provided they abide by the restrictions in Sections 2.2 and elsewhere in these Terms and Conditions of Use, for the following Permitted Uses. Permitted Uses may be undertaken within the premises of an Authorized User’s affiliated Institutional Licensee. Except in the case of Authorized Users who are Walk-In Users, Permitted Uses also may be undertaken remotely through secure access methods:

- (a) research activities;
- (b) classroom or organizational instruction and related classroom or organizational activities;
- (c) student assignments;
- (d) as part of a scholarly, cultural, educational, or organizational presentation or workshop, if such use conforms to the customary and usual practice in the field;
- (e) on an ad hoc basis and without commercial gain or in a manner that would substitute for direct access to the Content via services offered by JSTOR, sharing discrete Textual Content or Specimens with an individual who is not an Authorized User for purposes of collaboration, comment, or the scholarly exchange of ideas;
- (f) in research papers or dissertations, including reproductions of the dissertations, provided such reproductions are only for personal use, library deposit, and/or use solely within the institution(s) with which the Authorized User and/or his or her faculty readers are affiliated;
- (g) linking (see Section 2.3, below); and
- (h) Regarding Textual Content and Specimens, fair use under Section 107 of the U.S. Copyright Act, educational exceptions, or other similar provisions of the copyright laws or other intellectual property right laws in the United States or in other countries.

Should an Institutional Participation Agreement or other user agreement terminate or expire, the Institutional Licensee’s affiliated Authorized Users or other Authorized Users may continue making use of Textual Content and/or Specimens that have been downloaded or printed out

providing such uses comply with these Terms and Conditions of Use, which shall survive the termination of access under the Institutional Participation Agreement or other user agreement. .

**2.2 Prohibited Uses.** Institutions and users may not:

- (a) use or authorize the use of the JSTOR Platform or Content for commercial purposes or gains, including charging a fee-for-service for the use of JSTOR beyond reasonable printing or administrative costs. For purposes of clarification, “commercial purposes or gains” shall not include research whose end-use is commercial in nature;
- (b) except as set forth in Section 2.1(e) and 2.4, provide and/or authorize access to the Content available through Individual Access, the Publisher Sales Service, or other programs to persons or entities other than Authorized Users;
- (c) modify, obscure, or remove any copyright notice or other attribution included in the Content;
- (d) attempt to override, circumvent, or disable any encryption features or software protections employed in the JSTOR Platform;
- (e) Systematically print out or download Content to stock or replace print holdings;
- (f) undertake any activity that may burden JSTOR's server(s) such as computer programs that automatically download or export Content, commonly known as web robots, spiders, crawlers, wanderers or accelerators;
- (g) make any use, display, performance, reproduction, or distribution that exceeds or violates these Terms and Conditions of Use; or
- (h) incorporate Content into an unrestricted database or website, except that authors or other Content creators may incorporate their Content into such sites with prior permission from the publisher and other applicable rights holders;
- (i) download or print, or attempt to download or print: an entire issue or issues of journals or substantial portions of the entire run of a journal, other than on an isolated basis because of the relevance of the entire contents of a journal issue to a particular research purpose; or substantial portions of series of monographs or manuscripts; or
- (j) reproduce or distribute Content in bulk, such as by including Content in course packs, electronic reserves, repositories, or organizational intranets (but see Section 2.3, below).

**2.3 Linking.** JSTOR encourages the use of links to facilitate access to the Content by Authorized Users and Institutional Licensees, including but not limited to links to online syllabi, bibliographies, and reading lists. All Content has a stable URL that can be found in the Browse and Search interfaces of JSTOR's website as well as on the Article Information page for each discrete Content item. Further information on establishing stable links to material in JSTOR may be obtained from User Support ([support@jstor.org](mailto:support@jstor.org)).

**2.4 Interlibrary Loan.** Institutional Licensees may wish to use the Content for the purpose of fulfilling occasional requests from other libraries, a practice commonly called Interlibrary Loan. Institutional Licensees may use Licensed Content that consists of Textual Content or Specimens for Interlibrary Loan provided that such use is not at a volume that would substitute for a subscription to the journal or participation in JSTOR by the receiving institution and is in accordance with United States or international copyright laws, guidelines, or conventions. By way of example, Institutional Licensees shall comply with the CONTU Guidelines, available at <http://www.cni.org/docs/infopols/CONTU.html>, unless the Institutional Licensee is subject to similar international guidelines or customary and usual practices regarding Interlibrary Loan. Transmission of Licensed Content that consists of Textual Content or Specimens from one library to another (but not directly to users) through post or fax, or secure electronic transmission, such as Ariel or its equivalent, may be used in Interlibrary Loan. To facilitate direct contact with publishers for the provision of Textual Content outside the allowable scope of Interlibrary Loan

or for other permissions, Publisher contact information is available at <http://www.jstor.org/action/showJournals?browseType=publisherInfoPage>.

### 3. Intellectual Property Rights

3.1 General Intellectual Property Rights. The JSTOR Platform and any trademarks, issued patents and patent applications, copyrights and copyright registrations and applications, rights in ideas, designs, works of authorship, derivative works, and all other intellectual property rights (collectively, “Intellectual Property”) relating to the JSTOR Platform and its participating libraries, universities, publishers, scholarly societies, and journals are proprietary to JSTOR or, as applicable, the aforementioned entities, subject to the rights of third parties. Institutional Licensees and Authorized Users’ use of JSTOR implies no rights to Intellectual Property except for the limited rights set forth in these Terms and Condition of Use.

3.2 Trademarks. Neither JSTOR nor Institutional Licensee may use the other’s name or trademark(s) and Institutional Licensees and users may not use the name or trademark(s) of the above-noted entities in a way likely to cause confusion as to the origin of goods or services, or to endorse or show affiliation with the other, except as specifically approved. Notwithstanding the foregoing, (i) JSTOR may use Institutional Licensees’ names and/or the names of their libraries in brochures or other materials to identify Institutional Licensees as participants in JSTOR along with other participants, and (ii) Institutional Licensees are encouraged to use JSTOR’s name and logo to announce participation to Authorized Users and to train Authorized Users on the use of JSTOR.

3.3 Use of Software. JSTOR utilizes software and other electronic tools designed to permit Authorized Users to access, use, reproduce, display, and distribute Licensed Content (“Access Software”). Use of the Access Software and its related documentation is limited to the license granted herein. Institutional Licensees and users may not copy, distribute, modify, decompile, reverse engineer, circumvent, override or disable encryptions or other protections in, or create derivative works from the Access Software.

### Access, Support, and Security

#### 4.1 Responsibilities of JSTOR

4.1.1 JSTOR shall use reasonable efforts to provide continuous availability of the JSTOR Platform subject to periodic unavailability due to maintenance of the server(s), the installation or testing of software, the loading of journals as they become available, and downtime related to equipment or services outside the control of JSTOR, including public or private telecommunications services or internet nodes or facilities (“Maintenance Downtime”). If JSTOR fails to provide online availability to the JSTOR Platform for more than 72 hours during any period of 30 consecutive calendar days Institutional Licensee may, upon written request, (a) be granted its choice of a refund or a credit of a prorated portion of its annual access fee for each 30-day period so affected or (b) terminate its agreement by providing written notice to JSTOR.

4.1.2 JSTOR shall provide support to Institutional Licensees and Authorized Users in accordance with the terms set forth at <http://www.jstor.org/page/info/about/policies/support.jsp>.

4.1.3 JSTOR is committed to supporting and working with industry standards and best practices for online information delivery as these standards are developed. In furtherance of this commitment, JSTOR shall use reasonable efforts to ensure that:

4.1.3.1 the JSTOR Platform is compliant with Section 508 of the Rehabilitation Act and W3C WAI Priority 1 accessibility standards. Further information about JSTOR and accessibility is available at <http://www.jstor.org/page/info/resources/librarians/accessibility.jsp>;

4.1.3.2 the JSTOR Platform meets ANSI/NISO z39.88-2004 OpenURL standards;

4.1.3.3 the JSTOR Platform is compatible with the NISO Metasearch XML Gateway (MXG) protocol in development, XML and SRU/SRW search interfaces; and

4.1.3.4 it makes available to Institutional Licensees COUNTER-compliant usage statistics.

4.1.4 Subject to constraints imposed by or in agreement with journal publishers, JSTOR shall use reasonable efforts to ensure that the journals contained in the JSTOR Platform are complete and faithful replications of the print versions of such journals.

## 4.2 Responsibilities of Institutional Licensees

4.2.1 Institutional Licensees shall make reasonable efforts to ensure that access to the Licensed Content is limited to Authorized Users and to protect the Licensed Content from unpermitted use. Institutional Licensees shall notify JSTOR of any such unpermitted use of which they learn or are notified and shall cooperate with JSTOR in resolving problems of unpermitted use. In the event of violation of these Terms and Conditions of Use by an Authorized User, (a) JSTOR may suspend or terminate, or, where practicable, request that Institutional Licensee suspend or terminate, such Authorized User's access to the Licensed Content; (b) JSTOR may suspend or terminate the access of the Internet Protocol ("IP") address(es) or other authorization and authentication mechanisms from which such unauthorized use occurred; and/or (c) JSTOR may request Institutional Licensee to consider the imposition of further reasonable restrictions on access to, and downloading and printing from, the JSTOR Platform. JSTOR shall make reasonable efforts to contact the Institutional Licensee prior to any suspension or termination of access and to restore access promptly following successful resolution of the matter.

4.2.2 Access to the Platform shall be controlled by JSTOR through the use of IP addresses, Shibboleth, and/or, at JSTOR's sole discretion, passwords or other methods. Institutional Licensees shall be responsible for issuing and terminating passwords within its control, verifying the status of Authorized Users, providing lists of valid passwords or sets of IP addresses to JSTOR if applicable, and updating such lists on a regular basis.

4.2.3 The JSTOR Platform is intended to be accessible by telecommunications links between JSTOR's storage locations and Institutional Licensees' or Authorized Users' workstations or devices approved in advance in writing by JSTOR. Institutional Licensees and/or Authorized Users are responsible for establishing and maintaining hardware and Internet access to provide access to, and to transmit, the JSTOR Platform to Authorized Users. Institutional Licensees understand and agree that Internet browser software is required to access the JSTOR Platform. The Hardware and Software Requirements page available at <http://www.jstor.org/page/info/resources/librarians/tech.jsp#sysReqs> sets forth hardware

platforms and browsing software required and/or recommended for accessing the JSTOR Platform. Institutional Licensees and Authorized Users understand and agree that from time to time the Content may be added to or modified by JSTOR, that portions of the Content may migrate to other formats, and that the terms of the Hardware and Software Requirements page may be updated in a manner consistent with evolving industry standards. Institutional Licensees and Authorized Users shall be responsible for all costs associated with the use of and with establishing access to the JSTOR Platform, including but not limited to any telecommunications or other charges imposed by carriers, proprietary network operators and Internet access providers, or licenses for browser software, if any, as well as for all costs associated with printing from the JSTOR Platform.

#### 4.3 Responsibilities of Authorized Users

4.3.1 Authorized Users are responsible for maintaining the confidentiality and security of their username and/or password (if such are provided), and for all usage or activity by them of JSTOR. Except as permitted in Section 2.1(e), Authorized Users may not provide access to JSTOR to anyone else, including by setting up an anonymous remailer for purposes of allowing access to JSTOR.

4.3.2 Authorized Users promptly shall notify JSTOR and, where application, their affiliated Institutional Licensee, of any known or suspected unauthorized use(s) of their account or JSTOR, or any known or suspected breach of security, including loss, theft, or unauthorized disclosure or use of their username, password, and/or IP address. Any use of JSTOR beyond the scope or in violation of these Terms and Conditions of Use, knowing use of any password or username of another, or any fraudulent, abusive, or otherwise illegal activity, may be grounds for termination of an Authorized User's account, or termination of access to JSTOR from their IP address, without notice and at JSTOR's sole discretion.

#### 5. Warranty; Disclaimers

5.1 Authorized Users recognize that JSTOR is an aggregator of third-party Content, not the creator of the Content. JSTOR represents and warrants under the laws of United States that to its knowledge use of the JSTOR Platform and Licensed Content by Authorized Users in accordance with the terms of this Agreement shall not infringe the copyright of any third party. The foregoing shall not apply, however, to modifications or derivative works of the Content created by Institutional Licensees, Authorized Users or by any third party, nor usage of the JSTOR Platform or Content by Institutional Licensees or Authorized Users in violation of these Terms and Conditions of Use. *Please note that the foregoing further shall not apply to certain Collections. See Section 12 below for additional information.*

5.2 JSTOR shall not be liable, and Institutional Licensees and Authorized Users agree that they shall not hold JSTOR liable for any loss, injury, claim, liability, damages, costs, and/or attorneys fees of any kind that result from the unavailability of the JSTOR Platform or Content, delays or interruption of the services provided hereunder, or arising out of or in connection with Institutional Licensee's or Authorized Users' use of the JSTOR Platform or Content in violation of these Terms and Conditions of Use. If the JSTOR Platform fails to operate in conformance with the terms of this Agreement, Institutional Licensee shall immediately notify JSTOR, and, subject to Section 4.1.1 above, JSTOR's sole obligation shall be to repair the nonconformity. In no event shall JSTOR's liability to an Institutional Licensee exceed the fees paid to JSTOR by that Institutional Licensee for the term of the agreement then in effect.

**5.3 OTHER THAN ANY EXPRESS WARRANTIES STATED IN THIS SECTION 5, THE JSTOR PLATFORM, CONTENT, AND ACCESS SOFTWARE ARE PROVIDED ON AN "AS IS" BASIS, AND JSTOR AND ANY AND ALL THIRD PARTY CONTENT AND SOFTWARE PROVIDERS AND/OR LICENSORS ("CONTENT PROVIDERS") DISCLAIM ANY AND ALL OTHER WARRANTIES, CONDITIONS, OR REPRESENTATIONS OF ANY KIND (EXPRESS, IMPLIED, ORAL, OR WRITTEN) RELATING TO JSTOR, CONTENT, ACCESS SOFTWARE, OR ANY PARTS THEREOF, INCLUDING WITHOUT LIMITATION, ANY AND ALL IMPLIED WARRANTIES OF QUALITY, PERFORMANCE, COMPATIBILITY, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. JSTOR AND ALL CONTENT PROVIDERS MAKE NO WARRANTIES WITH RESPECT TO ANY HARM THAT MAY BE CAUSED BY THE TRANSMISSION OF A COMPUTER VIRUS, WORM, TIME BOMB, LOGIC BOMB, OR OTHER SUCH COMPUTER PROGRAM, EXCEPT THAT JSTOR WILL EXERCISE A REASONABLE LEVEL OF CARE TO PREVENT SUCH OCCURRENCES. JSTOR AND ALL CONTENT PROVIDERS FURTHER DISCLAIM ANY LIABILITY AND MAKE NO WARRANTIES WITH RESPECT TO ANY ERRORS OR OMISSIONS IN THE CONTENT, LIABILITY UNDER LIBEL LAWS, INFRINGEMENT OF RIGHTS OF PUBLICITY AND PRIVACY, MORAL RIGHTS, OR THE DISCLOSURE IN THE CONTENT OF CONFIDENTIAL INFORMATION AND FURTHER DISCLAIM ANY LIABILITY AND MAKE NO WARRANTY WITH RESPECT TO ANY CLAIMS AND/OR THREATENED CLAIMS (INCLUDING INTELLECTUAL PROPERTY RIGHTS CLAIMS AND/OR THREATENED CLAIMS) RELATING TO: LINKS BETWEEN THE JSTOR PLATFORM AND OTHER SITES AND/OR THE CONTENT ON SUCH LINKED SITES; ADAPTATIONS AND/OR MODIFICATIONS OF CONTENT; ANY AND ALL USES, REPRODUCTIONS, DISPLAYS, PERFORMANCES, AND DISTRIBUTIONS THAT EXCEED THE PERMITTED USES (WHETHER PERMITTED BY LAW OR OTHERWISE); AND/OR ANY USE(S), REPRODUCTIONS, DISPLAYS, PERFORMANCES, AND DISTRIBUTIONS MADE OF CONTENT (PRINTED OR EXPORTED) AFTER THE EXPIRATION OR TERMINATION OF THIS AGREEMENT AND/OR THE APPLICABLE INSTITUTIONAL PARTICIPATION AGREEMENT.**

6. Withdrawing Content from JSTOR. JSTOR may withdraw Content from JSTOR for good cause shown. JSTOR would endeavor, to the extent practicable, to minimize any inconvenience to Authorized Users caused by such withdrawal by, for example, seeking to withdraw Content only at the conclusion of an academic semester. However, should JSTOR be unable to avoid such inconvenience, JSTOR in no way shall be held liable for the withdrawal of such Content from the JSTOR Platform. If JSTOR withdraws a material amount of Content, Institutional Licensee may, upon written request, (a) be granted its choice of a refund or a credit of a prorated portion of its annual access fee for the Agreement then in effect or (b) terminate its agreement without penalty by providing written notice to JSTOR.

7. Privacy Policy. Use of JSTOR indicates acceptance of [JSTOR's Privacy Policy](http://www.jstor.org/page/info/about/policies/privacy.jsp), available at <http://www.jstor.org/page/info/about/policies/privacy.jsp> as it may be amended from time to time.

8. Force Majeure. Neither JSTOR nor Institutional Licensees or Authorized Users shall be liable for failures or delays in performing their obligations pursuant to this contract arising from any cause beyond their control, including but not limited to, act of God, acts of civil or military authority, terrorism, fires, strikes, lockouts or labour disputes, epidemics, wars, riots, earthquakes, storms, typhoons and floods and in the event of any such delay, the time for either party's



performance shall be extended for a period equal to the time lost by reason of the delay. If the conditions giving rise to the delay continue beyond thirty (30) consecutive days, either party may terminate its agreement with the other by giving written notice to the other party.

## 9. General

9.1 These Terms and Conditions of Use are, where applicable, subject to and incorporated by reference into Institutional Licensees' Institutional Participation Agreements. In the event of any conflict between these Terms and Conditions of Use and the Institutional Participation Agreement applicable to an Institutional Licensee and/or Authorized User, the Institutional Participation Agreement shall prevail. Please contact your librarian for further details concerning your Institutional Participation Agreement, if you are affiliated with an Institutional Licensee. Information identifying Institutional Licensees is available at <http://www.jstor.org/page/info/about/organization/participantLists/participantsAll.jsp>.

9.2 These Terms and Conditions of Use shall be interpreted and construed according to United States Federal law, excluding any such laws or conventions that might direct the application of the laws of another jurisdiction, and venue shall lie exclusively in the federal and state courts of the United States, excluding any such laws to the contrary.

9.3 If any provision or provisions of these Terms and Conditions of Use shall be held to be invalid, illegal, unenforceable, or in conflict with the law of any jurisdiction, the validity, legality, and enforceability of the remaining provisions shall not be in any way affected or impaired thereby. A waiver of any breach of these Terms and Conditions of Use shall not be deemed a waiver of other breaches of these Terms and Conditions of Use.

9.4 The English language version of agreements with JSTOR shall be controlling over any other version.

9.5 These Terms and Conditions of Use are for the sole benefit of the parties to these Terms and Conditions of Use and are not intended for the benefit of any third party. The parties expressly disclaim the creation of any third party beneficiary rights under these Terms and Conditions of Use.

## 10. Archiving and Post Cancellation Access

10.1 Archiving of Back Issues. As an archive serving the scholarly community, JSTOR provides long term preservation of the Back Issue material in its collections. Back Issue materials are journal volumes and issues dated behind the "Moving Wall" or older manuscripts and monographs. For further information about the Moving Wall, please see <http://www.jstor.org/page/info/about/archives/journals/movingWall.jsp>. Institutional Licensees typically pay two types of fees to JSTOR for Back Issue materials, an Annual Access Fee and an Archive Capital Fee. The Annual Access Fee is a periodic payment covering the Institutional Licensee's access to the JSTOR Platform. The Archive Capital Fee is one-time fee per JSTOR collection aimed at ensuring the long term preservation, upgrading, and enhancements of the scholarly materials in the JSTOR Platform. By paying the Archive Capital Fee to support a JSTOR collection, Institutional Licensees are securing reliable, long term preservation, upgrading, and enhancements of the Back Issue material in that collection for their institution. Should an Institutional Licensee elect to terminate access to a JSTOR Back Issue collection, it may resume access to that Back Issue collection and all content subsequently added to that

collection at any time in the future through payment of only the Annual Access Fee. It would not need to re-pay the Archive Capital Fee.

JSTOR recognizes that preserving scholarly material requires those entities responsible to employ best practices in preservation as well as to provide assurances about the security of the material and the organization's long term viability as a trusted archive. JSTOR pursues best practices and standards in the creation and maintenance of the JSTOR Platform, has established mirror sites and multiple back up files for all of the materials in the JSTOR Platform, and demonstrates its ability to provide continuing access on a daily basis. Additionally, for those Back Issue materials included in the JSTOR Platform that have print editions, JSTOR has established dedicated repositories at several participating institutions to house and preserve the print copies under archival-quality conditions. With the support of Institutional Licensees, JSTOR is also developing an endowment to ensure the long term operating viability of the JSTOR Platform.

**10.2 Post Cancellation Access:** Access to Current Issues shall be available to Institutional Licensees following the Institution's cancellation or non-renewal of a subscription to the Current Issues of the applicable journal ("Post Cancellation Access"). Current Issues materials are those issues of journal(s) published online back to the Digital Availability Date. The "Digital Availability Date" is the year when issues of the Journal(s) initially were published online in digital format, subject to exceptions as determined by the publisher and JSTOR. For purposes of clarification, the Digital Availability Date does not refer to when digitized versions of print issues became available as a JSTOR archival product but rather refers to when "born digital" versions of the title became available. Information concerning the Digital Availability Date for each title is available at <http://support.jstor.org/csp/titles/>. The scope of an Institution's Post Cancellation Access may include the following options:

- **Current Issues and Back Issues Content:** As noted in 10.1 above, institutions that continue to license Back Issues for applicable fees, whether in connection with a single publication subscription or a collection subscription, are assured of Post-Cancellation Access to issues of the journal "behind" the Moving Wall, which will advance annually. In addition, JSTOR will honor access to subscribed Current Issues for cancelled or non-renewed Subscriptions until the Moving Wall catches up to the year in which the Subscription was cancelled or discontinued.
- **Through Portico:** All of the journals whose Current Issues are available on the JSTOR Platform are also part of the Portico digital preservation service, which may include Post Cancellation Access under the terms set forth in the Portico Journal Archive License Agreement. Institutions participating in Portico may use this mechanism for obtaining Post Cancellation Access to a cancelled Current Issues journal.
- **Per-Publication Post Cancellation Access:** For Licensed Institutions for which neither of the above Post Cancellation options applies, JSTOR will provide Post Cancellation Access to subscribed Current Issues content for a small annual fee.

**11. Terms and Conditions Subject to Change.** In the interest of managing the evolving needs of Institutional Licensees, Authorized Users, and Content providers, JSTOR reserves the right to modify these Terms and Conditions, or any aspect of JSTOR, at any time. The most updated Terms and Conditions of Use will be posted on the JSTOR website. JSTOR shall notify Institutional Licensees via email of material modifications. A modification shall become effective for an Institutional Licensee if it does not object in writing to JSTOR within 60 (sixty)



days from the time JSTOR emails notice of the modification. In the event of such an objection, the Institutional Licensee shall have the right to terminate the Agreement on 30 (thirty) days written notice.

12. Additional Terms and Conditions of Use. Please see below for Terms and Conditions of Use specific to certain Collections or Content:

12.1 Institutions in the United Kingdom and Republic of Ireland, and their users please see [http://www.jisc-collections.ac.uk/catalogue/ireland\\_resources/how\\_to\\_subscribe](http://www.jisc-collections.ac.uk/catalogue/ireland_resources/how_to_subscribe) for The Ireland Collection.

12.2 Institutions in the United Kingdom and their users please see [http://www.jisc-collections.ac.uk/catalogue/19th\\_pamphlets/how\\_to\\_subscribe](http://www.jisc-collections.ac.uk/catalogue/19th_pamphlets/how_to_subscribe) for the 19<sup>th</sup> Century British Pamphlets Collection.

12.3 For the *African Plants, Cultural Heritage Sites and Landscapes*, and *Struggles for Freedom in South Africa* Collections, please see <http://www.jstor.org/page/info/about/policies/additionalTerms.jsp> addressing accessibility standards and Section 5.1 of these Terms and Conditions of Use.

12.4 For the *Current Scholarship Program*, please see <http://www.jstor.org/page/info/about/policies/csp.jsp> addressing Section 5.1 of these Terms and Conditions of Use.


Last Updated on July 1, 2010

MIT Network Dynamic Host Registration

MIT Network Dynamic Host Reg... +

mit.edu https://nic.mit.edu:444/bin/dynareg

MIT Networks Network Contacts PGP B G GR GD GM GW YouTube YT DHCP ITSS WIKI EPO IdF Drops locations /b/ Computing Infra... View On Black Bookmarks



Dynamic Host Configuration

## Visitor Registration

Please fill out the form below. You can use this registration for up to 14 days per year before you are required to formally register with us. If your registration expires and less than 14 days have been used, you will be diverted back to this form for an extension.

name:  Please do not include apostrophes

email:  limit of 32 characters

phone:

name of person/department you are visiting or event you are attending:

number of days (use 1 unless you know you will use the network for multiple consecutive days):


faq | [feedback](#)

MIT Network Dynamic Host Registration

MIT Network Dynamic Host Reg... +

mit.edu https://nic.mit.edu:444/bin/dynareg?class=visitor

MIT Networks Network Contacts PGP B G GR GD GM GW YT DHCP ITSS WIKI EPO IdF Drops locations /b/ Computing Infra... View On Black Bookmarks



Dynamic Host Configuration

## Registering Your Computer

This registration will allow you to temporarily use the network as a visitor. By registering your computer, you are agreeing to the MITnet rules of use.

- Don't let anyone know your password(s).
- Don't violate the privacy of other users.
- Don't interfere with the integrity of the system.
- Don't copy or misuse copyrighted material (including software).
- Don't use the network to harass anyone in any way.
- Don't restrict or deny access to the network by legitimate users.
- Don't use the network for private financial gain.

Please understand and follow the rules of use. Violations will result in loss of network service.

[Register](#)

faq | [feedback](#)

[For Faculty & Staff](#) [For Students](#) [For IT Support Providers](#)

GET STARTED WITH IT	OUR SERVICES	SOFTWARE & HARDWARE	SECURE COMPUTING	ABOUT IS&T

# MITnet Rules of Use

## On this page:

[Overview](#)[Summary](#)[MITnet Rules of Use](#)[Intended Use](#)[Ethical Use](#)[Proper Use](#)

## Overview

MITnet, MIT's campus-wide computer network, connects the MIT community and our guests to thousands of workstations, servers, printers, mobile devices and electronic resources of every kind located on and off campus. Network connectivity has many advantages which you will discover as you explore MITnet, and the Internet beyond. But connectivity also requires that users of the network understand their responsibilities in order to protect the integrity of the system and the privacy of other users.

This section summarizes the rules that apply to all users of MITnet. We expect you to follow all these rules, and we hope you will encourage others to follow them as well.

To report someone willfully violating the rules, send email to [stopit@mit.edu](mailto:stopit@mit.edu). If you believe you are in danger, call the [Campus Police](#) *immediately* at x3-1212.

## Summary

The listing below provides only summaries of the rules. For the full text of each rule, please see the following pages.

### MITnet Rules of Use

#### *Comply with Intended Use of the System*

1. Don't violate the intended use of MITnet.

#### *Assure Ethical Use of the System*

2. Don't let anyone know your password(s).
3. Don't violate the privacy of other users.
4. Don't misuse the intellectual property of others.
5. Don't use MITnet to harass anyone in any way.

#### *Assure Proper Use of System Resources*

6. Don't misuse electronic communications and collaboration services.

## MITnet Rules of Use

MITnet and other computing resources at MIT are shared among community members. The MITnet Rules of Use are intended to help members of the MIT community use MIT's computing and network facilities responsibly, safely, and efficiently, thereby maximizing the availability of these facilities to community members. Complying with them will help maximize access to these facilities, and assure that all use of them is responsible, legal, and respectful of privacy. If you have questions or wish further information about any of the MITnet policies outlined below, send email to [security@mit.edu](mailto:security@mit.edu).

All network users are expected to follow these rules. ***Violations of the rules can subject the offender to Institute disciplinary proceedings, loss of network privileges, and, in some cases, civil or criminal prosecution.***

**NOTE:** Laws that apply in "the real world" also apply in the "virtual" networked computer world (including MITnet). Laws about libel, harassment, privacy, copyright, stealing, threats, etc. are *not* suspended for computer users, but apply to all members of society whatever medium they happen to be using: face-to-face, phone, *or* computer. Furthermore, law-enforcement officials are more computer-savvy than ever, and violations of the law in "Cyberspace" are vigorously prosecuted.

Similarly, Institute policies (as described in MIT's [Policies and Procedures](#), for example) also apply to MITnet users.

## Complying With the Intended Use of the System

It is important that you understand the purpose of MITnet so that your use of the system is in compliance with that purpose.

### 1. Don't violate the intended use of MITnet.

The purpose of MITnet is to support research, education, and MIT administrative activities, by providing access to computing resources and the opportunity for collaborative work. All use of the MIT network must be consistent with this purpose. For example:

- *Don't try to interfere with or alter the integrity of the system at large*, by doing any of the following:
  - permitting another individual to use your account
  - impersonating other individuals in communication  
(particularly via forged email, texts, instant messages and social media postings)
  - attempting to capture or crack passwords or encryption
  - destroying or altering data or programs belonging to other users
- *Don't try to restrict or deny access to the system by legitimate users.*
- *Don't use MITnet for private financial gain.* For example, users are *not* permitted to run a private business on MITnet. (Commercial activity *is* permitted, but *only* for business done on behalf of MIT or its organizations. Cf. Section 13.2.3 of MIT's [Policies and Procedures](#): "MIT's computing and telecommunications facilities and services are to be used for Institute purposes only and not for the benefit of private individuals or other organizations without authorization.")
- *Don't transmit threatening or harassing materials.* (Cf. [Rule 5](#).)

## Assuring Ethical Use of the System

Along with the many opportunities that MITnet provides for members of the MIT community to share information comes the responsibility to use the system in accordance with MIT standards of honesty and personal conduct. Those standards, outlined in Section 13.2 of MIT's [Policies and Procedures](#), call for all members of the community to act in a responsible, professional way.

Appropriate use of MITnet resources includes maintaining the security of the system, protecting privacy, and conforming to applicable laws, particularly copyright and harassment laws.

### 2. Don't let anyone know your password(s).

While you should feel free to let others know your username (this is the name by which you are known to the whole Internet user community), you should *never* let anyone know your account passwords. This includes even trusted friends, and computer system administrators (e.g., IS&T staff).

Giving someone else your password is like giving them a signed blank check, or your charge card. You should never do this, even to "lend" your account to them temporarily. Anyone who has your password can use your account, and whatever they do that affects the system will be traced back to your username -- if your username or account is used in an abusive or otherwise inappropriate manner, you can be held responsible.

In fact, there is never any reason to tell anyone your password: every MIT student, faculty member, or on-campus staff person who wants an account of his or her own can have one. And if your goal is permitting other users to read or write some of your files, there are always ways of doing this without giving away your password.

For information about how to manage the security of your account, including advice on how to choose a good password, see [IS&T: Security](#) and [IT Security: Passwords](#).

### **3. Don't violate the privacy of other users.**

The Electronic Communications Privacy Act (18 USC 2510 *et seq.*, as amended) and other federal laws protect the privacy of users of wire and electronic communications.

The facilities of MITnet encourage sharing of information. Security mechanisms for protecting information from unintended access, from within the system or from the outside, are minimal. These mechanisms, by themselves, are not sufficient for a large community in which protection of individual privacy is as important as sharing (see, for example, sections 11.2, 11.3, and 13.2 of MIT's [Policies and Procedures](#)). Users must therefore supplement the system's security mechanisms by using the system in a manner that preserves the privacy of themselves and others.

As Section 11.1 of MIT's *Policies and Procedures* notes, "Invasions of privacy can take many forms, often inadvertent or well-intended." All users of MITnet should make sure that their actions don't violate the privacy of other users, if even unintentionally.

Some specific areas to watch for include the following:

- *Don't try to access the files or directories of another user without clear authorization from that user.* Typically, this authorization is signaled by the other user's setting file-access permissions to allow public or group reading of the files. If you are in doubt, ask the user.

- *Don't try to intercept or otherwise monitor any network communications not explicitly intended for you.* These include logins, e-mail, user-to-user dialog, and any other network traffic not explicitly intended for you.
- Unless you understand how to protect private information on a computer system, *don't use the system to store personal information about individuals which they would not normally disseminate freely about themselves* (e.g., grades, address information, etc.)
- *Don't make any personal information about individuals publicly available without their permission.* This includes both text and number data about the person (biographical information, phone numbers, etc.), as well as representations of the person (graphical images, video segments, sound bites, etc.) For instance, it is *not* appropriate to include a picture of someone on a World Wide Web page without that person's permission. (Depending on the source of the information or image, there may also be copyright issues involved; cf. [Rule 4](#)).
- *Don't create any shared programs that secretly collect information about their users.* Software on MITnet is subject to the same guidelines for protecting privacy as any other information-gathering project at the Institute. (This means, for example, that you may not collect information about individual users without their consent.)
- *Don't remotely log into (or otherwise use) any workstation or computer not designated explicitly for public logins over the network -- even if the configuration of the computer permits remote access -- unless you have explicit permission from the owner and the current user of that computer to log into that machine.*

#### **4. Don't misuse the intellectual property of others.**

MIT faculty, students, and staff produce and consume a vast amount of intellectual property, much of it in digital form, as part of our education and research missions. This includes materials covered by the patent, copyright, and trademark laws, as well as license or other contractual terms.

Members of the MIT community also avail themselves of a wide variety of entertainment content that is available on the Internet, most of which is protected by copyright or subject to other legal restrictions on use.

All users need to insure that their use of all these protected digital materials respects the rights of the owners.

Digital materials that may be covered by this rule, without limitation, are:

- Data
- E-books
- Games



- Journals and periodicals
- Logos
- Movies
- Music
- Photographs and other graphics
- Software
- Textbooks
- Television programs
- Other forms of video content

You should assume that all materials are subject to these legal protections, and may have some restrictions on use. Ease of access, downloading, sharing, etc. should not be interpreted as a license for use and re-distribution.

Of particular concern is the prevalence of peer-to-peer file sharing as a medium for the unauthorized exchange of copyrighted materials, including movies, music, games, and other software programs. As required by the [Higher Education Opportunity Act](#), MIT has developed and implemented a written plan to effectively combat the unauthorized distribution of copyrighted materials by users of MIT's network. For more information, see [Copyright at MIT](#).

## **5. Don't use MITnet to harass anyone in any way.**

"Harassment," according to MIT's [Policies and Procedures](#) (Section 9.5), is defined as:

"...any conduct, verbal or physical, on or off campus, which has the intent or effect of unreasonably interfering with an individual or group's educational or work performance at MIT or that creates an intimidating, hostile or offensive educational, work or living environment.... Harassment on the basis of race, color, gender, disability, religion, national origin, sexual orientation or age includes harassment of an individual in terms of a stereotyped group characteristic, or because of that person's identification with a particular group."

The Institute's harassment policy extends to the networked world. For example, sending email or other electronic messages which unreasonably interfere with anyone's education or work at MIT may constitute harassment and is in violation of the intended use of the system.

Any member of the MIT community who feels harassed is encouraged to seek assistance and resolution of the complaint. To report incidents of on-line harassment, send email to [abuse@mit.edu](mailto:abuse@mit.edu). If you believe you are in danger, call the Campus Police *immediately* at x3-1212.

## Assuring Proper Use of the System

MITnet's resources, as well as the resources MITnet gives you access to (e.g., computing facilities, email and calendaring services, instant messaging, wikis, the web), are powerful tools that provide maximum benefit to the entire MIT community when used reasonably and in manners consistent with the intended uses of those resources.

### **6. Don't misuse electronic communications and collaboration services.**

MIT provides electronic communications and collaboration services to members of the MIT community. These services include, but are not limited to, electronic mail, mailing lists, instant messaging, message boards, websites, wikis, blogs, social networking sites, forums, collaborative spaces, Voice over IP (VoIP) and video services.

Some members of the MIT community access similar, or additional, 3rd party services on the Internet.

Users of all such services have a responsibility to use these services properly and to respect the rights of others in their use of these services, and in accordance with published terms of service.

Users may not use these services in violation of any applicable law.

All relevant [MIT policies](#) apply to the use of these services, but in particular:

- Any use that might contribute to the creation of a hostile academic or work environment is prohibited,
  - Any commercial use not required for coursework, research or the conduct of MIT business is prohibited,
  - Any non-incidental personal use such as advertisements, solicitations or promotions is prohibited
- [Note: some services exist on campus that have been designed for buying, selling and exchanging items within the MIT community, and those are allowed].

MIT Senior Leadership has authorized certain individuals to send electronic mail to large groups such as all Faculty, all employees, all undergraduates, Class of 2012, etc, or to the entire MIT community. These lists are not open to posts from the community at large. Contact the owners of these lists for further information.

Users should understand a service's policies prior to use. Service operators and providers should, to the extent feasible, publish their terms of service.

Any content posted to a service that is inconsistent with these rules, as well as unsolicited mail from outside of MIT (e.g., SPAM), may be subject to automated interception, quarantine and disposal.

## RELATED PAGES AND HOW TO

[Athena Rules of Use](#)

[Athena Computing Environment](#)

[Athena User Accounts](#)

[Athena Consulting](#)

[Obtaining an Athena Workstation](#)

[The Athena Release](#)

Massachusetts  
Institute of Technology

Information Services and Technology |  
617.253.1101  
[Ask the Help Desk](#) or contact the [IS&T Webmasters](#).

---

FOR FACULTY & STAFF

---

FOR STUDENTS

---

FOR VISITORS

---

FOR IS&T STAFF

---

FOLLOW US

---

# Guerilla Open Access

## *Manifesto*

**Information is power.** But like all power, there are those who want to keep it for themselves. The world's entire scientific and cultural heritage, published over centuries in books and journals, is increasingly being digitized and locked up by a handful of private corporations. Want to read the papers featuring the most famous results of the sciences? You'll need to send enormous amounts to publishers like Reed Elsevier. There are those struggling to change this. *The Open Access Movement* has fought valiantly to ensure that scientists do not sign their copyrights away but instead ensure their work is published on the Internet, under terms that allow anyone to access it. But even under the best scenarios, their work will only apply to things published in the future. Everything up until now will have been lost.

That is too high a price to pay. Forcing academics to pay money to read the work of their colleagues? Scanning entire libraries but only allowing the folks at Google to read them? Providing scientific articles to those at elite universities in the First World, but not to children in the Global South? It's outrageous and unacceptable.

"I agree," many say, "but what can we do? The companies hold the copyrights, they make enormous amounts of money by charging for access, and it's perfectly legal — there's nothing we can do to stop them." But there is something we can, something that's already being done: we can fight back.

Those with access to these resources — students, librarians, scientists — you have been given a privilege. You get to feed at this banquet of knowledge while the rest of the world is locked out. But you need not — indeed, morally, you cannot — keep this privilege for yourselves. You have a duty to share it with the world. And you have: trading passwords with colleagues, filling download requests for friends.

Meanwhile, those who have been locked out are not standing idly by. You have been sneaking through holes and climbing over fences, liberating the information locked up by the publishers and sharing them with your friends.

But all of this action goes on in the dark, hidden underground. It's called stealing or piracy, as if sharing a wealth of knowledge were the moral equivalent of plundering a ship and murdering its crew. But sharing isn't immoral — it's a moral imperative. Only those blinded by greed would refuse to let a friend make a copy.

Large corporations, of course, are blinded by greed. The laws under which they operate require it — their shareholders would revolt at anything less. And the politicians they have bought off back them, passing laws giving them the exclusive power to decide who can make copies.

There is no justice in following unjust laws. It's time to come into the light and, in the grand tradition of civil disobedience, declare our opposition to this private theft of public culture.

We need to take information, wherever it is stored, make our copies and share them with the world. We need to take stuff that's out of copyright and add it to the archive. We need to buy secret databases and put them on the Web. We need to download scientific journals and upload them to file sharing networks. We need to fight for *Guerilla Open Access*.

With enough of us, around the world, we'll not just send a strong message opposing the privatization of knowledge — we'll make it a thing of the past. Will you join us?  
July 2008, Eremo, Italy



http://guerillaopenaccess.com/

Go

SEP JAN FEB

Close X

9 captures

22 Sep 08 - 3 Feb

2009 2011 2012

Help ?

## Guerilla Open Access *Manifesto*

Information is power. But like all power, there are those who want to keep it for themselves. The world's entire scientific and cultural heritage, published over centuries in books and journals, is increasingly being digitized and locked up by a handful of private corporations. Want to read the papers featuring the most famous results of the sciences? You'll need to send enormous amounts to publishers like Reed Elsevier.

There are those struggling to change this. *The Open Access Movement* has fought valiantly to ensure that scientists do not sign their copyrights away but instead ensure their work is published on the Internet, under terms that allow anyone to access it. But even under the best scenarios, their work will only apply to things published in the future. Everything up until now will have been lost.

That is too high a price to pay. Forcing academics to pay money to read the work of their colleagues? Scanning entire libraries but only allowing the folks at Google to read them? Providing scientific articles to those at elite universities in the First World, but not to children in the Global South? It's outrageous and unacceptable.

"I agree," many say, "but what can we do? The companies hold the copyrights, they make enormous amounts of money by charging for access, and it's perfectly legal — there's nothing we can do to stop them." But there is something we can, something that's already being done: we can fight back.

Those with access to these resources — students, librarians, scientists — you have been given a privilege. You get to feed at this banquet of knowledge while the rest of the world is locked out. But you need not — indeed, morally, you cannot — keep this privilege for yourselves. You have a duty to share it with the world. And you have: trading passwords with colleagues, filling download requests for friends.

Meanwhile, those who have been locked out are not standing idly by. You have been sneaking through holes and climbing over fences, liberating the information locked up by the publishers and sharing them with your friends.

But all of this action goes on in the dark, hidden underground. It's called stealing or piracy, as if sharing a wealth of knowledge were the moral equivalent of plundering a ship and murdering its crew. But sharing isn't immoral — it's a moral imperative. Only those blinded by greed would refuse to let a friend make a copy.

Large corporations, of course, are blinded by greed. The laws under which they operate require it — their shareholders would revolt at anything less. And the politicians they have bought off back them, passing laws giving them the exclusive power to decide who can make copies.

There is no justice in following unjust laws. It's time to come into the light and, in the grand tradition of civil disobedience, declare our opposition to this private theft of public culture.

We need to take information, wherever it is stored, make our copies and share them with the world. We need to take stuff that's out of copyright and add it to the archive. We need to buy secret databases and put them on the Web. We need to download scientific journals and upload them to file sharing networks. We need to fight for *Guerilla Open Access*.

With enough of us, around the world, we'll not just send a strong message opposing the privatization of knowledge — we'll make it a thing of the past. Will you join us?

*July 2008, Eremo, Italy*

### join the fight

**the mailing list:** learn, discuss, help.

**content liberation front:** the guerillas of the open access movement.

**public.resource.org:** liberating US government documents.

**downhill battle:** the war against file sharing is not one you can win.

**theinfo.org:** for people who like large data sets.

(did we miss you? tell the mailing list.)

(cc) share and enjoy



## Host Lookup

### visitor registration

name:

email:

phone:

days remaining: 9

last expiration date: 29-Sep-2010

MAC address:

status: ☐ active ☒ inactive

comment:  
please include  
contact info

record last updated by mhalsall@mit.edu at Thu Sep 30 12:57:46 2010 EDT

[Delete Host](#) [Update Host](#)

[faq](#) | [feedback](#)



Activity in MITnet computer registration database

Fields:  
mac, status, account, bcontact, tcontact, ace\_type, ace, visit\_name, visit\_email, visit\_phone, visit\_sponsor, visit\_course, visit\_class, visit\_total, visit\_expires, comment, created\_dt, created\_tm, created\_by, modified\_dt, modified\_tm, modified\_by

Registration on Sept. 24:  
INSERT INTO host\_less VALUES ('00235a735ffb',0,'visitor',NULL,NULL,0,0,'Gary Host','ghost@mailinator.com','','',NULL,NULL,5,'29-Sep-2010','', '24-Sep-2010','22:46:19',0,'30-Sep-2010','12:57:46',182635)Wg

Registration on Oct. 2:  
INSERT INTO host\_less VALUES ('00235a735ffc',0,'visitor',NULL,NULL,0,0,'Gary Host','ghost42@mailinator.com','','',NULL,NULL,10,'13-Oct-2010','', '02-Oct-2010','10:20:37',0,'13-Oct-2010','05:54:22',182635)Wg

Registration on Oct. 8:  
INSERT INTO host\_less VALUES ('0017f22cb074',0,'visitor',NULL,NULL,0,0,'Grace Host','ghost42@mailinator.com','','',NULL,NULL,5,'13-Oct-2010','', '08-Oct-2010','22:13:26',0,'14-Oct-2010','10:45:57',182635)Wg

Registration on Oct. 22:  
INSERT INTO host\_less VALUES ('004ce5a0c755',1,'visitor',NULL,NULL,NULL,NULL,'Grace Host','ghost42@mailinator.com','','',NULL,NULL,10,'11-Nov-2010','', '22-Oct-2010','21:39:30',0,'06-Nov-2010','22:12:19',0)Wg

Registration on Nov. 28:  
INSERT INTO host\_less VALUES ('004ce5a0c756',1,'visitor',NULL,NULL,NULL,NULL,'Grace Host','ghost42@mailinator.com','','',NULL,NULL,2,'07-Jan-2011','', '28-Nov-2010','18:29:19',0,'06-Jan-2011','12:44:43',0)Wg

Activity in DHCP logs corresponding to computer registration database

ghost.txt:dhcpllogger/dhcp-20100925.gz:Sep 24 22:45:35 installer dhcpcd: DHCPOFFER on 18.2.55.247 to 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1



ghost.txt:dhcpllogger/dhcp-20100930.gz:Sep 29 01:31:29 installer dhcpcd: DHCPOFFER on 18.2.55.247 to 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1

ghost.txt:dhcpllogger/dhcp-20100930.gz:Sep 29 01:39:52 installer dhcpcd: DHCPOFFER on 18.2.55.247 to 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1

ghost.txt:dhcpllogger/dhcp-20101001.gz:Sep 30 18:11:25 installer dhcpcd: DHCPOFFER on 18.2.55.247 to 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1

ghost.txt:dhcpllogger/dhcp-20101003.gz:Oct 2 10:20:07 installer dhcpcd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1

ghost.txt:dhcpllogger/dhcp-20101003.gz:Oct 2 10:20:50 installer dhcpcd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1

ghost.txt:dhcpllogger/dhcp-20101003.gz:Oct 2 10:20:54 installer dhcpcd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1

ghost.txt:dhcpllogger/dhcp-20101003.gz:Oct 2 10:26:44 installer dhcpcd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1

ghost.txt:dhcpllogger/dhcp-20101003.gz:Oct 2 10:27:06 installer dhcpcd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1

ghost.txt:dhcpllogger/dhcp-20101003.gz:Oct 2 10:27:52 installer dhcpcd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1

ghost.txt:dhcpllogger/dhcp-20101003.gz:Oct 2 10:28:45 installer dhcpcd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1

ghost.txt:dhcpllogger/dhcp-20101003.gz:Oct 2 10:29:29 installer dhcpcd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1

ghost.txt:dhcpllogger/dhcp-20101003.gz:Oct 2 10:30:29 installer dhcpcd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1

ghost.txt:dhcpllogger/dhcp-20101008.gz:Oct 7 01:49:06 installer dhcpcd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1

ghost.txt:dhcpllogger/dhcp-20101009.gz:Oct 8 22:12:09 installer dhcpcd: DHCPOFFER on 18.2.55.166 to 00:17:f2:2c:b0:74 (ghost-macbook) via 18.55.0.1

ghost.txt:dhcpllogger/dhcp-20101009.gz:Oct 8 22:15:06 installer dhcpcd: DHCPOFFER on 18.2.55.166 to 00:17:f2:2c:b0:74 (ghost-macbook) via 18.55.0.1

ghost.txt:dhcpllogger/dhcp-20101009.gz:Oct 8 22:58:57 installer dhcpcd: DHCPOFFER on 18.2.55.212 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1

ghost-laptop\_dhcp\_01062011.txt:dhcp-20110107.gz:Jan 6 12:42:49 installer dhcpcd: DHCPOFFER on 18.2.53.219 to 00:4c:e5:a0:c7:56 (ghost-laptop) via 18.53.0.1





10000  
AUTOMATIC  
CAUTION  
DOOR

10000  
AUTOMATIC  
CAUTION  
DOOR

AUTOMATIC DOOR  
NO PUSH BUTTON

Building  
16

M.I.T.

Private Property

No Trespassing

No Soliciting

Trespassers and Solicitors

will be subject to prosecution

459



**Building  
16**

**M.I.T.**

**Private Property**

**No Trespassing**

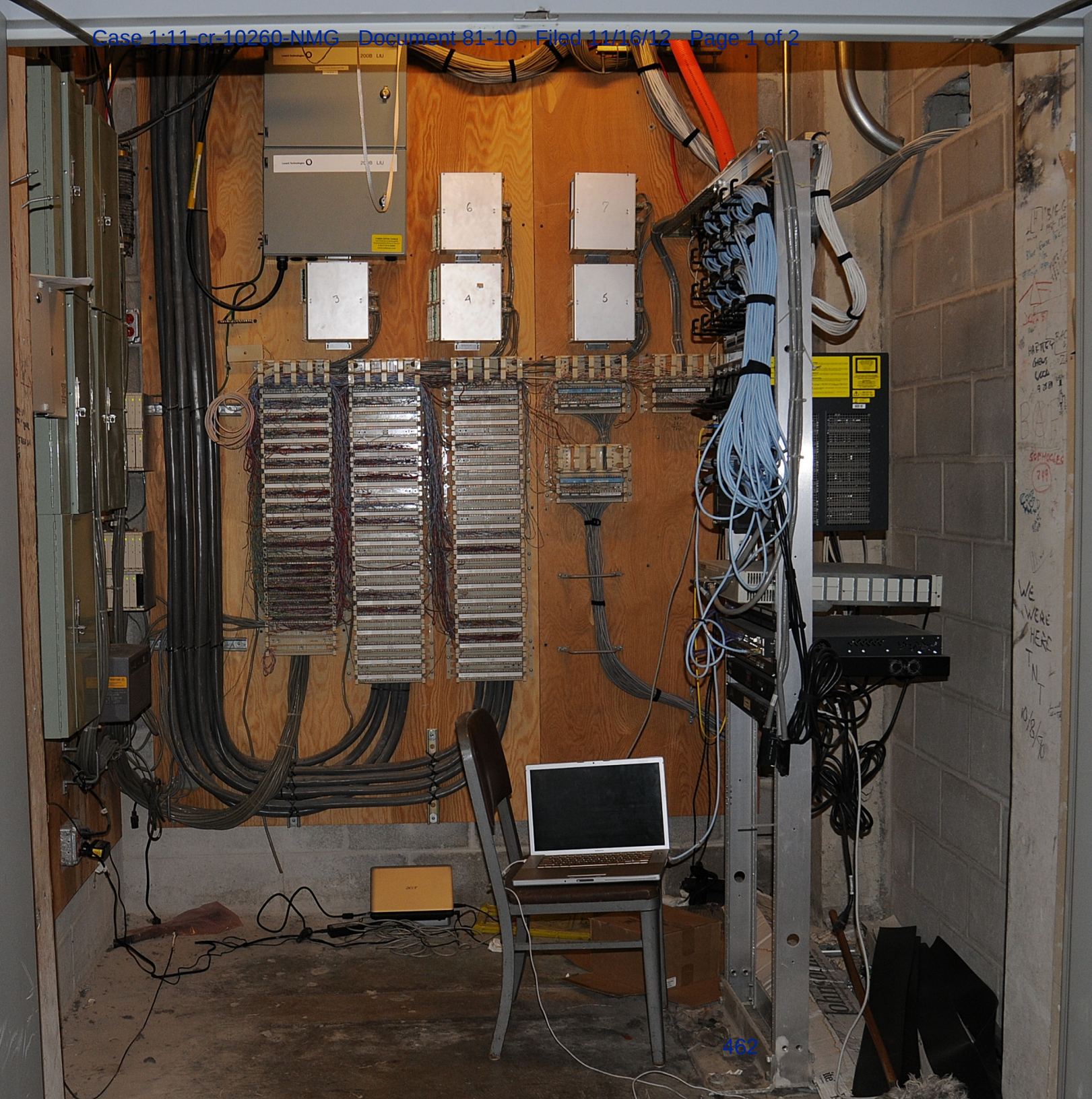
**No Soliciting**

**Trespassers and solicitors  
will be subject to prosecution.**











BOX CERTIFICATE

ULINE

WE HAVE ALL THE EQUIPMENT AND SUPPLIES YOU NEED FOR YOUR BUSINESS

200

1000

1000

JAN 1963

JAN 1963





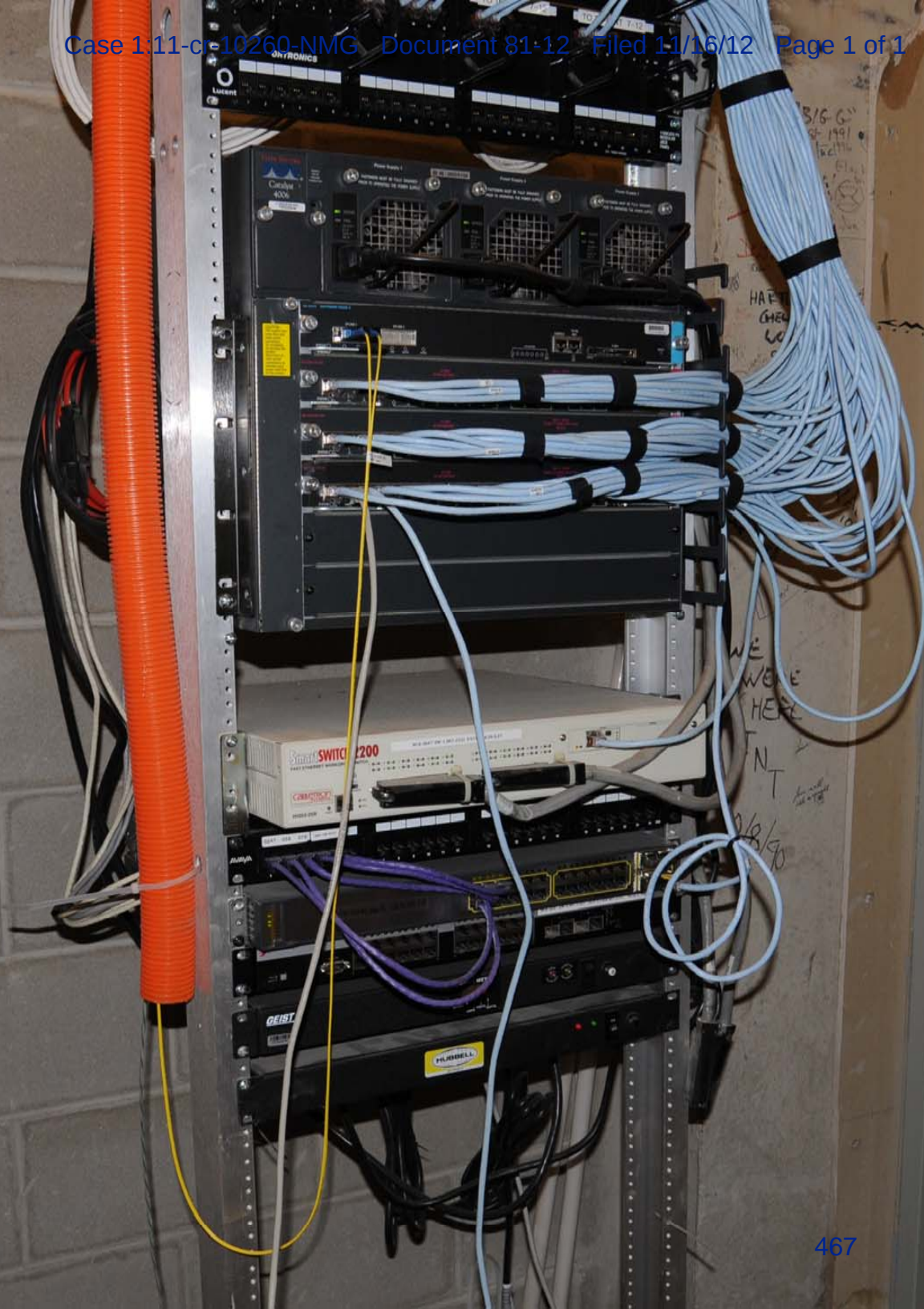


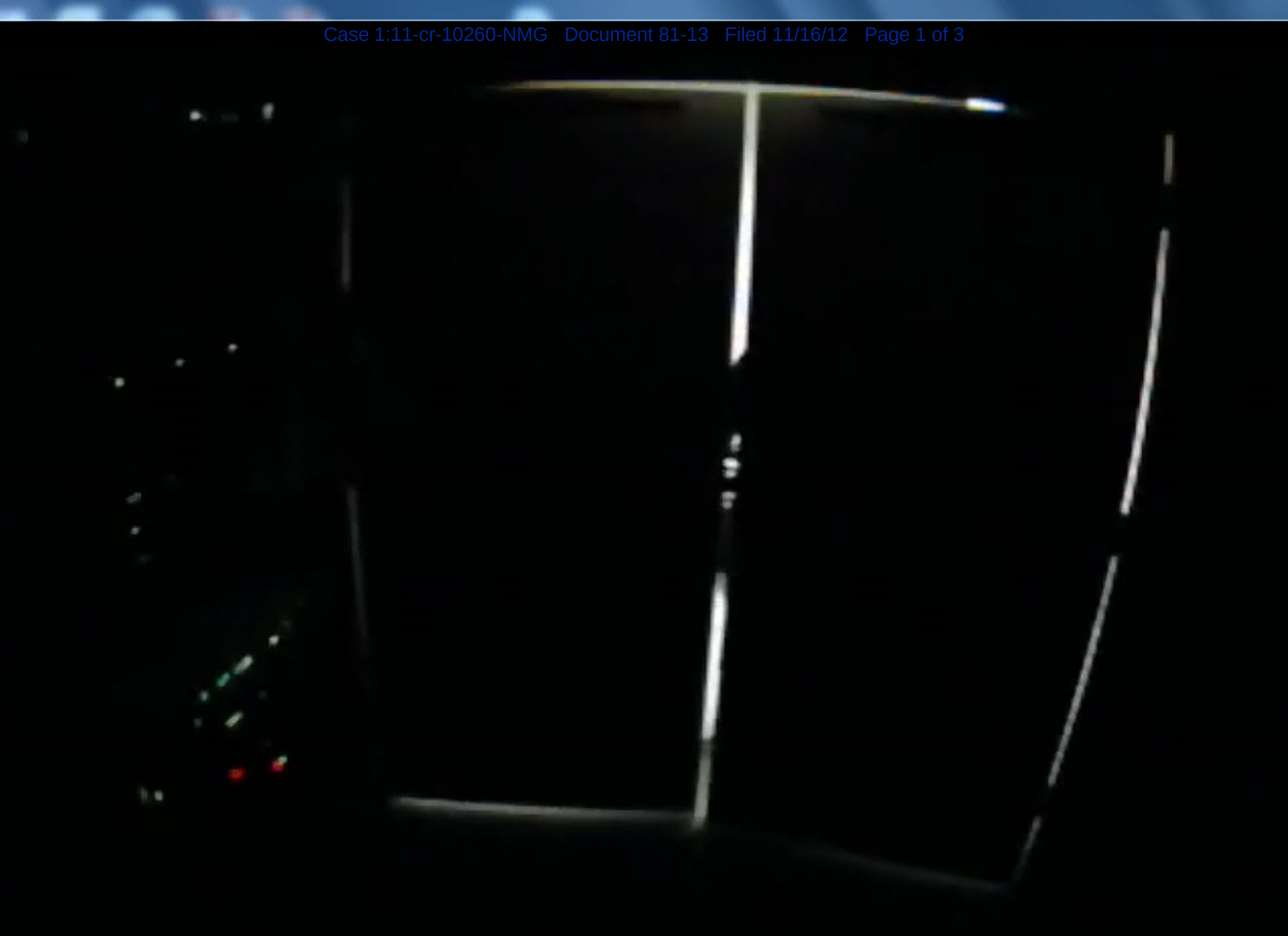












00:47



468







470

00:53

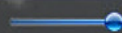








03:57



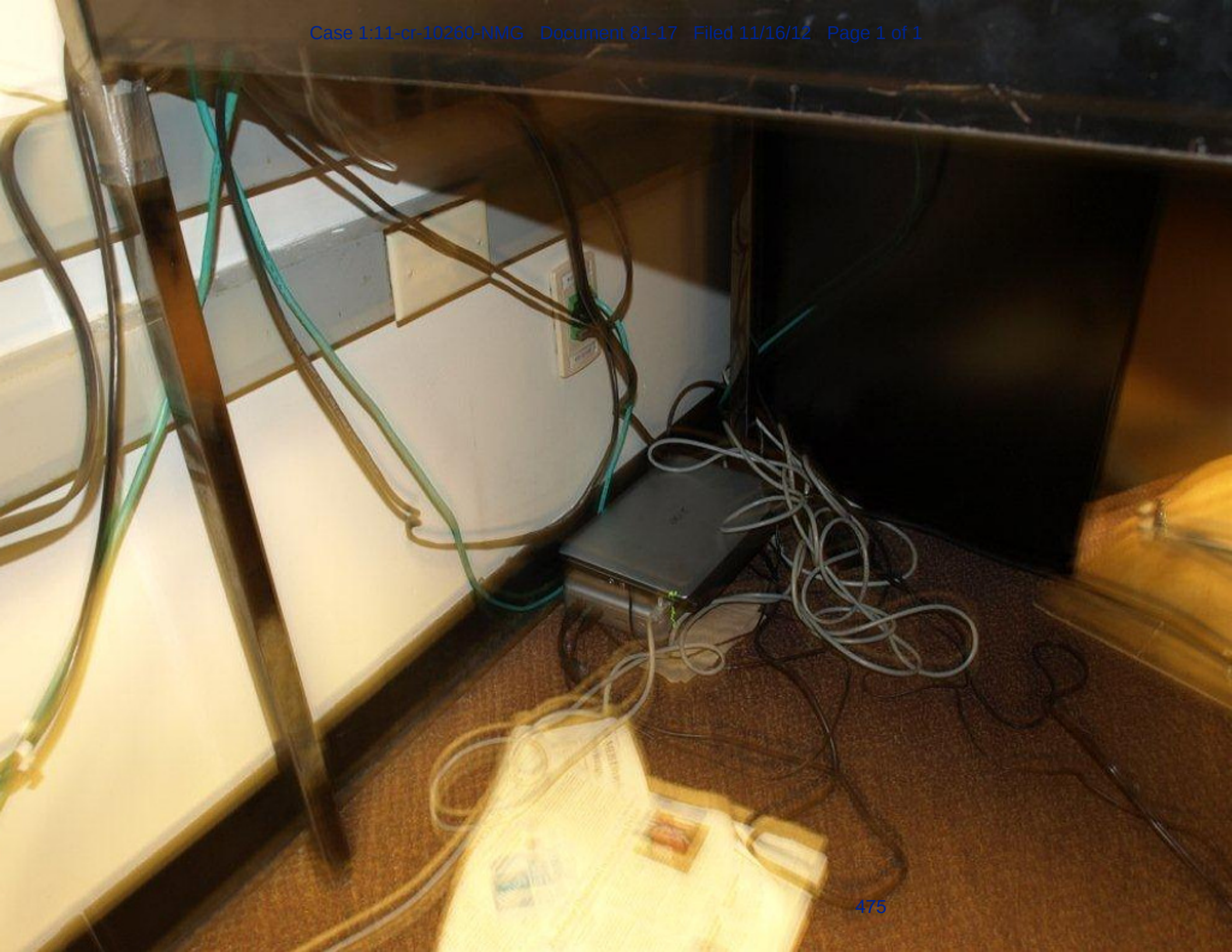
472











[For Faculty & Staff](#) [For Students](#) [For IT Support Providers](#)



GET STARTED WITH IT	OUR SERVICES	SOFTWARE & HARDWARE	SECURE COMPUTING	ABOUT IS&T

# IS&T Policies: DHCP Usage Logs Policy

[About IS&T](#) > [IT Policies](#) > [IS&T Policies: DHCP Usage Logs Policy](#)

[Get Help](#)

## On this page:

[Policy](#)

[Rationale](#)

[Implementation](#)

[Implications](#)

[Glossary](#)

[History](#)

## Policy

IS&T records a variety of information about both the operation and/or use of its network services. When used in conjunction with IS&T's Host Registration database, records contained in logs showing the use of dynamic IP addresses on MITnet allow IS&T staff to follow up on problems, incidents, and inquiries.

These logs are retained for 30 days after their creation date. All of these logs are considered confidential, and as such IS&T takes active measures to prevent unauthorized access during the retention period.

Circumstances may arise where a log, or more usually a very small subset of one day's log, may need to be kept for longer than 30 days and, potentially, disclosed to certain third parties. The use of any such retained information by authorized staff, and the release of any log information to third parties, are done under the direction and with the approval of MIT's Office of the General Counsel.

This IS&T policy is limited to the Dynamic Host Configuration Protocol (DHCP) services and logs created in connection with MITnet. It does not apply to DHCP services or logs created by other Departments, Labs & Centers (DLCs) at MIT. IS&T recommends that other IT groups at MIT create similar policies that are based on business practices and are consistent with the needs and desires of those DLCs.

## Rationale

This policy implements MIT's Privacy Policy specifically for the collection and retention of DHCP logs. In setting the retention period, IS&T has weighed a variety of competing interests, chiefly the need to maintain robust operational reliability of MIT's network, the need to be responsive to third parties who report issues that we need to investigate or resolve, and the desire to limit log retention to reduce opportunities for inadvertent disclosure of operational data.

## Implementation

The DHCP server is configured to provide dynamic addresses automatically as needed. The logs of information are maintained on an IS&T-managed server. Each log is tagged with its creation date; once a day, the system deletes logs that are 30 days old.

When any network device, e.g., a computer, connects to MITnet and is assigned a dynamic IP address, MIT's DHCP server adds a record to its log containing the following information:

- The date and time of the request
- The MAC address of the requesting device or computer
- The IP address provided
- The specific DHCP command that was issued
- Other technical information related to the request

In the event of a request relating to a potential legal proceeding, IS&T staff may create a case in Request Tracker and store subsets of a log pertinent to the case at hand in the case record.

The DHCP server is in a secure location and complies with secure data storage best practices. IS&T's Network Services Infrastructure team acts as the data custodian for DHCP logs, and ensures that the logs are stored securely and are deleted when they expire.

The DHCP logs capture only one type of network usage. Related, but not addressed in this policy, are Virtual Private Network (VPN) usage logs, hostnames/static IP addresses usage logs, or dialup usage logs, among others.

## Implications

Retaining and securing DHCP usage logs as described above are necessary to ensure that the confidentiality of the DHCP lease logs is protected but that the information in the logs is still available as needed to ensure MITnet's security and integrity.

MIT is required to comply with a court order or valid subpoena that requests the disclosure of information contained in DHCP logs. Failure to comply could have serious consequences for the individuals, IS&T, and the Institute. MIT's Office of the General Counsel is qualified and authorized to confirm that a request for information contained in logs is legitimate and not an improper attempt to gain access to confidential information.

## Glossary

**DHCP:** Dynamic Host Configuration Protocol. This protocol defines the process by which a device can dynamically receive an IP address from a pool of addresses, instead of requiring the device to have a fixed IP address. This is ideal for devices like laptops, which will not all be connected to the network at all times from the same location.

**Dynamic IP Address:** When a device has not been assigned a Static IP address, an Internet service provider will assign an address at the time the device is connecting to the Internet.

**IP Address:** Internet Protocol (IP) Address. See references below for more information on network addressing.

**DLCs:** A collective term meant to describe the common elements among MIT's many academic, administrative and research units, while acknowledging the many differences amongst MIT units.

**Static IP Address:** A number (in the form of a dotted quad) that is assigned to a network device or computer by an Internet service provider (ISP) which will be its permanent address on the Internet.

**VPN:** [Virtual Private Network](#). A technology that in MIT's usage facilitates secure communications from remote locations to a known location at MIT, typically over the public Internet. However, VPNs are not inherently about security or performance, but rather that they provide a "tunnel" on top of some other network in support of a given customer or client community.

## History

**Status:** In effect

**Policy Steward:** Paul Acosta

**Policy Owner:** Marilyn T. Smith

**RELATED PAGES AND HOW  
TO**[IT Policies](#)[Virtual Private Network \(VPN\)](#)[MITnet Bootstrap Registration](#)[MIT Privacy and Disclosure of  
Information Policy](#)

---

[ABOUT IS&T](#)

---

[NEWS](#)

---

[OUR ORGANIZATION](#)

---

[MISSION & STRATEGIC PLAN](#)

---

[IT POLICIES](#)

---

[IT GOVERNANCE](#)

---

[JOB OPENINGS](#)

---

Massachusetts  
Institute of Technology

Information Services and Technology |  
617.253.1101  
[Ask the Help Desk](#) or contact the [IS&T  
Webmasters](#).

---

[FOR FACULTY & STAFF](#)

---

[FOR STUDENTS](#)

---

[FOR VISITORS](#)

---



FOR IS&T STAFF

---

FOLLOW US

---



Date/Time Printed: 01-07-2011 09:34:45

Version 2.0 - 11/05

<b>CRIMINAL COMPLAINT</b> ORIGINAL		DOCKET NUMBER 1152CR000073	NO. OF COUNTS 1	<b>Trial Court of Massachusetts District Court Department</b>
DEFENDANT NAME & ADDRESS Aaron H Swartz 349 Marshman Ave. Highland Park, IL 60035				COURT NAME & ADDRESS Cambridge District Court 4040 Mystic Valley Parkway Medford, MA 02155 (781)306-2710
DEFENDANT DOB 11/08/1986	COMPLAINT ISSUED 01/07/2011	DATE OF OFFENSE 01/04/2011	ARREST DATE 01/06/2011	<b>ARREST</b>
OFFENSE CITY / TOWN Cambridge		OFFENSE ADDRESS		
POLICE DEPARTMENT M.I.T Campus Police		POLICE INCIDENT NUMBER 11000351		NEXT EVENT DATE & TIME 01/07/2011 9:00 AM
OBTN TCAM201100032				NEXT SCHEDULED EVENT Arraignment
ROOM / SESSION Arraignment Session				
The undersigned complainant, on behalf of the Commonwealth, on oath complains that on the date(s) indicated below the defendant committed the offense(s) listed below and on any attached pages.				

COUNT	CODE	DESCRIPTION
1	266/18/B	B&E BUILDING DAYTIME FOR FELONY c266 §18

On 01/04/2011 did in the day time break and enter a ship, motor vehicle or vessel, the property of MIT & Jstor.com, with intent to commit a felony, in violation of G.L. c.266, §18.

PENALTY: state prison not more than 10 years; or jail not more than 2 years and not more than \$500. District Court has final jurisdiction under G.L. c.218, §26.

SIGNATURE OF COMPLAINANT <i>X / G. Swartz</i>	SWORN TO BEFORE CLERK-MAGISTRATE/ASST. CLERK/DEP. ASST. CLERK <i>X / Robert D. Dwyer</i>	DATE 1-7-11
NAME OF COMPLAINANT <i>Craig A. Martin</i>	CLERK-MAGISTRATE/ASST. CLERK <i>X</i>	DATE

Notice to Defendant: 42 U.S.C. § 3796gg-4(e) requires this notice: If you are convicted of a misdemeanor crime of domestic violence you may be prohibited permanently from purchasing and/or possessing a firearm and/or ammunition pursuant to 18 U.S.C. § 922 (g) (9) and other applicable related Federal, State, or local laws.



**M.I.T. POLICE**  
**301 VASSAR ST CAMBRIDGE, MA**

INCIDENT # / REPORT #      OFFICER      RANK      REVIEW STATUS  
 11000351 / 1      JPERAULT      DETECTIVE      APPROVED by JPERAULT

**INCIDENT #11000351 DATA**

As Of 01/06/2011 16:19:21

**BASIC INFORMATION**

<u>CASE TITLE</u>	<u>LOCATION</u>	<u>AFT/UNIT</u>	<u>CITY, STATE</u>
B&E	21 AMES ST		CAMBRIDGE, MA
<u>DATE/TIME REPORTED</u>	<u>DATE/TIME OCCURRED</u>		
01/06/2011 14:20:45	On or after 01/04/2011 15:26		
<u>INCIDENT TYPE/OFFENSE</u>			
B&E DAYTIME FOR FELONY c266 S18			

**PERSONS**

<u>ROLE</u>	<u>NAME</u>	<u>SEX</u>	<u>RACE</u>	<u>AGE</u>	<u>DOB</u>	<u>PHONE</u>
VICTIM	MIT,					(HOME)
	ADDRESS: [REDACTED]		CAMBRIDGE, MA			(CELL)

**OFFENDERS**

<u>STATUS</u>	<u>NAME</u>	<u>SEX</u>	<u>RACE</u>	<u>AGE</u>	<u>DOB</u>	<u>PHONE</u>
DEFENDANT	SWARTZ, AARON H	MALE	UNKNOWN	24	[REDACTED]	(HOME)
	ADDRESS: , IL					(CELL)

[ NO VEHICLES ]

**PROPERTY**

<u>CLASS</u>	<u>DESCRIPTION</u>	<u>MAKE</u>	<u>MODEL</u>	<u>SERIAL #</u>	<u>VALUE</u>
--------------	--------------------	-------------	--------------	-----------------	--------------

**OFFICER REPORT: 11000351 - 1 / JPERAULT (DETECTIVE)**

<u>DATE/TIME OF REPORT</u>	<u>TYPE OF REPORT</u>	<u>REVIEW STATUS</u>
01/06/2011 14:20:45	INCIDENT	APPROVED

**NARRATIVE**

On January 4, 2010 at approximately 10:30 hours I responded to MIT building 16, room 004T for a report of a past break. This room is a telephone closet and networking closet; it's access is controlled by MIT's IS&T Department. David Newman of MIT IS&T explained to me that someone had entered the restricted room and connected a laptop and external hard drive directly to a networking switch. The

laptop and external hard drive were being hidden under a cardboard box. Newman further explained that they were able to determine that this laptop was illegally downloading scientific periodicals from JStor, a subscription based database that houses academic periodicals.

Cambridge Police Detective Joseph Murphy, Special Agent Michael Pickett from the United States Secret Service and Boston Police Officer Tim Laham responded to building 16 room 004T. Cambridge Police's Crime Scene Services also responded and processed the laptop and external hard drive for latent prints. It was determined that the laptop would be left in place and IS&T would monitor the network traffic in an attempt to identify the suspect. A camera was also installed by MIT's IS&T Department to monitor the area.

On January 4, 2010 at approximately 15:26 hours a white male, dark or black shoulder length wavy hair, wearing a dark coat, gray backpack, jeans with a white bicycle helmet enters the room. It appears as though the suspect takes a hard drive out of his back pack and bends over the laptop and external hard drive. He exits the room moments later.

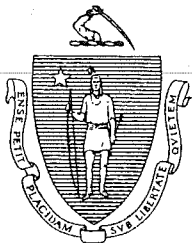
On January 5, 2010 MIT's IS&T Department informed me that approximately 70 gigabytes of data had been downloaded, 98% of which was from JStor. SA Mike Pickett had informed me that MIT's IS&T had put an approximate value on the downloaded information at \$50,000.

On January 6, 2010 at approximately 12:32 hours a white male, dark or black shoulder length wavy hair, wearing a dark coat, gray backpack, jeans with a white bicycle helmet enters the room. I was monitoring the video feed at the MIT Police Department at this time. It appears as though the suspect packed up the laptop and hard drive and exited the room. MIT Police units responded to the area and searched for the suspect. A check of the room determined that the laptop and hard drive had been removed.

On January 6, 2010 at approximately 14:11 hours Captain Albert Pierce of the MIT Police Department called me and stated he had located the suspect riding his bike on Massachusetts Ave at Lee Street. Special Agent Pickett and I responded to the Lee Street to assist Captain Pierce. The suspect jumped off his bike when encountered by Captain Pierce and ran down Lee Street. Captain Pierce and Special Agent Pickett were able to apprehend the suspect at 24 Lee Street. He was handcuffed by SA Pickett.

The suspect encountered by Captain Pierce and apprehended on Lee Street is the same person seen on video entering the restricted telephone closet in building 16 on January 4th at 15:26 hours and on January 6th at 14:11 hours.

He was arrested for two counts of Breaking and Entering in the daytime with the intent to commit a felony, Chapter 266 Section 18.



*The Commonwealth of Massachusetts*

HOUSE OF REPRESENTATIVES  
STATE HOUSE, BOSTON 02133

KENNETH M. LEMANSKI  
8TH HAMPDEN DISTRICT

ROOM 443, STATE HOUSE  
TEL. 722-2460

May 24, 1983

Mr. Richard Kendall  
Governor's Legislative Office  
State House - Room 381  
Boston, MA 02133

Dear Mr. Kendall:

Thank you for the opportunity to comment on H.6227, which revises the definition of "property" with respect to larceny.

The most important aspect of this bill, in my opinion, is the fact that it now allows electronic impulses to be defined as property. This is essential in combatting computer crime. As I am sure the Governor is aware, the Commonwealth is extremely dependent on computers of all types, business, academic and so on. H.6227 will give prosecutors what former Senator Ribicoff once called "wiggly room". That is, they will now be able to refer to a specific statute in the prosecution of what was formerly one of the most difficult types of crime. H.6227 directly attacks what, up until now, had been the judicial sticking point: are electronic data "property"? Our own Supreme Judicial Court agreed with earlier Federal opinions that the answer was no, under the existing statutes. H.6227 remedies this by explicitly including computer data in the definition of property.

The second section of H.6227 extends this definition to trade secrets, with the same intent. This is especially important when one stops to think of how much sensitive business data is contained in computers.

The Governor would be taking a great step toward furthering Massachusetts' reputation as a commercially and technologically progressive State by signing H.6227. I urge him most strongly to do so.

Thank you again for this opportunity, and please notify me of any signing.

Sincerely,

A handwritten signature in dark ink, appearing to read "Ken", written over a horizontal line.

Kenneth M. Lemanski  
STATE REPRESENTATIVE

KML/v

**SEARCH WARRANT**  
HP USB drive,  
marked 0045SMKBT1 85102

**Case No. 11M-5063-JGD**



## UNITED STATES DISTRICT COURT

for the  
District of MassachusettsIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

HP USB drive, marked 0045SMKBT1 85102

Case No.

11M-5863-J6D

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search  
of the following person or property located in the \_\_\_\_\_ District of \_\_\_\_\_ Massachusetts

(identify the person or describe the property to be searched and give its location):

HP USB drive, marked 0045SMKBT1 85102, as described in Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the  
property to be seized):evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1030(a)(2), 18 U.S.C. § 1030(a)(5)(A) and  
18 U.S.C. § 1343 (wire fraud,) as described in Attachment BI find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or  
property.

YOU ARE COMMANDED to execute this warrant on or before

March 10, 2011

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m.☐ at any time in the day or night as I find reasonable cause has been  
established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property  
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the  
place where the property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an  
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge  
Judith G. Dein

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay  
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be  
searched or seized (check the appropriate box) ☐ for \_\_\_\_\_ days (not to exceed 30).☐ until, the facts justifying, the later specific date of \_\_\_\_\_.

Date and time issued:

2/24/11 3:05



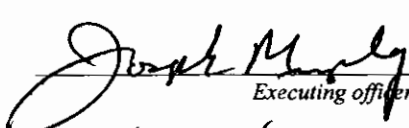
Judge's signature

City and state: Boston, Massachusetts

Chief U.S. Magistrate Judge Judith G. Dein

Printed name and title

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

<b>Return</b>		
Case No.: <b>11M-5063-JGD</b>	Date and time warrant executed: <b>2/25/2011 9:00 AM</b>	Copy of warrant and inventory left with: <b>KEVIN CAVANAUGH</b>
Inventory made in the presence of: <b>Property Technician Kevin Cavanaugh &amp; Dep. Sup. Joseph Wilson</b>		
Inventory of the property taken and name of any person(s) seized:  <div style="margin-top: 20px;"> <p><b>(1) HP USB Drive</b></p> <p><b>marked <del>00</del> 459 MKBT1 85102</b></p> </div>		
<b>Certification</b>		
<p><i>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</i></p>		
Date: <b>3/4/11</b>	<div style="text-align: center;">   <small>Executing officer's signature</small> </div> <div style="text-align: center; margin-top: 10px;"> <b>Joseph Murphy Special Fed Dep US Marshal</b>  <small>Printed name and title</small> </div>	



**Attachment A**

HP USB drive, marked 0045SMKBT1 85102

**ATTACHMENT B**

**ITEMS TO BE SEIZED**

- I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1030(a)(2) (intentionally accessing a computer without authorization and obtaining information with a value that exceeds \$5,000), 18 U.S.C. §1030(a)(5)(A) (intentionally causing damage without authorization to a protected computer) and 18 U.S.C. § 1343 (wire fraud), including, without limitation:
  - A. Records and tangible objects pertaining to the following entities, websites, computer networks, and IP addresses:
    1. JSTOR
    2. Massachusetts Institute of Technology
    3. Jstor.org
    4. Mit.edu
    5. IP addresses in the class A domain 18.
  - B. Records and tangible objects pertaining to the following topics:
    1. JSTOR
    2. Records and data digitized by JSTOR, including, without limitation, journals digitized by JSTOR
    3. Records and data stored on JSTOR
    4. Records and data originating on JSTOR
    5. Means of access to JSTOR
    6. Computer software capable of making repeated requests for data and records from JSTOR
    7. Computer software capable of making repeated downloads of records and data from JSTOR

8. MIT's computer network
  9. MIT's physical plant
  10. Remote electronic storage locations
  11. MAC addresses
- C. Records and tangible objects pertaining to the existence and identity of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the crimes listed above;
- D. Records and tangible objects pertaining to communications to any third parties in anticipation, during or following the crimes listed above about those crimes;
- E. Records and tangible objects relating to the ownership, occupancy, or use of 950 Massachusetts Avenue, Apartment 320, Cambridge, Massachusetts 02139 and assigned storage locker "C4", Acer Aspire One laptop computer, serial number LUSAX0D001001100E1601, 2.0 terabyte Western Digital hard drive, serial number WMAZA1626675, and HP USB drive, marked 0045SMKBT1 85102; and
- F. For any computer hardware, computer software, computer-related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):
1. evidence of who used, owned, or controlled the computer equipment;
  2. evidence of computer software that would allow remote access and control of the computer equipment
  3. evidence of the attachment of other computer hardware or storage

- media;
  - 4. evidence of counter-forensic programs and associated data that are designed to eliminate data;
  - 5. evidence of the times the computer equipment was used;
  - 6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment; and
  - 7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media.
- II. All computer hardware, computer software, computer-related documentation, and storage media. Off-site searching of these items shall be limited to searching for the items described in paragraph I.

#### **DEFINITIONS**

For the purpose of this warrant:

- A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.
- B. "Computer hardware" means any electronic device capable of data processing (such as a computer, personal digital assistant, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
- C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility,

communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

- D. "Computer-related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
- E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).
- F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.
- G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

## ATTACHMENT C

### **PROCEDURES FOR SEIZING COMPUTERS AND RELATED DEVICES**

#### **1. Seizing hardware and software**

Agents are authorized to seize and remove from the premises the computer hardware, software, related documentation, and storage media, so that computer analysts can accurately retrieve the items authorized by this warrant in a laboratory or other controlled environment. The retrieval process does not need to be completed within 14 days after the date of the warrant or before the return of the written inventory required by Fed. R. Crim. P. 41(a).

#### **2. Returning hardware and software**

If, after inspecting a seized computer system, the agents and computer analysts determine that these items are no longer necessary to retrieve and preserve electronic evidence, the prosecutor determines that they need not be preserved as evidence, fruits or instrumentalities of a crime, and these items do not contain contraband, they should be returned within a reasonable time, upon written request.

If the computer system cannot be returned, agents should, upon written request, make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that are neither the fruits nor instrumentalities of crime nor contraband.

**APPLICATION FOR  
SEARCH WARRANT**  
HP USB drive,  
marked 0045SMKBT1 85102

**Case No. 11M-5063-JGD**



# UNITED STATES DISTRICT COURT

for the  
District of Massachusetts

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

HP USB drive, marked 0045SMKBT1 85102

Case No. 11M-5063-JED

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

HP USB drive, marked 0045SMKBT1 85102, as described in Attachment A

located in the \_\_\_\_\_ District of \_\_\_\_\_ Massachusetts \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1030(a)(2), 18 U.S.C. § 1030(a)(5)(A) and 18 U.S.C. § 1343 (wire fraud,) as described in Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

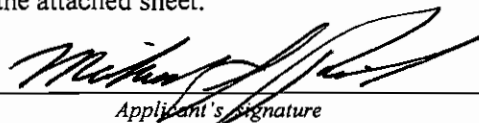
The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. Sec. 1030(a)(2)	intentionally accessing a computer without authorization and obtaining information
18 U.S.C. Sec. 1030(a)(5)(A)	intentionally causing damage without authorization to a protected computer
18 U.S.C. Sec. 1343	wire fraud

The application is based on these facts:  
See attached Affidavit of Special Agent Michael S. Pickett

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

Secret Service Special Agent Michael S. Pickett  
Printed name and title

Sworn to before me and signed in my presence

Date: 2/24/11



  
Judge's signature

City and state: Boston, Massachusetts

Chief U.S. Magistrate Judge Judith G. Dein  
Printed name and title

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Michael S. Pickett, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search an Acer Aspire One laptop computer, serial number LUSAX0D001001100E1601 ("the ACER LAPTOP"), a 2.0 terabyte Western Digital hard drive, serial number WMAZA1626675 ("the WESTERN DIGITAL HARD DRIVE"), and an HP USB drive, marked 0045SMKBT1 85102 ("the USB DRIVE"), as described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the United States Secret Service ("the Secret Service"), Department of Homeland Security, and have been since 2003. My current duties include the investigation of electronic crimes and forensic examination of computers and cellular telephones. As an agent, I have participated in numerous investigations involving computer and high technology related crimes, including computer intrusions, Internet fraud and credit card fraud. I also have received specialized training in the investigation of crimes involving unauthorized intrusions into computer networks. In connection with my official responsibilities, I am charged with investigating violations of 18 U.S.C. §§ 1030 and 1343.

3. As set forth herein, there is probable cause to believe that the ACER LAPTOP, the WESTERN DIGITAL HARD DRIVE, and the USB DRIVE contain evidence, instrumentalities, and fruits of violations of 18 U.S.C. § 1030(a)(2) (intentionally accessing a computer without authorization and obtaining information with a value that exceeds \$5,000), 18 U.S.C. §1030(a)(5)(A) (intentionally causing damage without authorization to a protected computer) and 18 U.S.C. § 1343 (wire fraud).

4. I make this affidavit based upon communications with witnesses and others with knowledge of the events, conversations with Secret Service agents, Cambridge Police, and MIT police, my review of records gathered in the course of the investigation described below and my

own observations and knowledge. Because this affidavit is intended to show only that there is probable cause for the requested warrants, it does not set forth all aspects of the investigation of which I or other Secret Service agents are aware.

#### **TECHNICAL TERMS**

5. Based on my experience, I use the following technical terms to convey the following meanings for the purpose of this affidavit:

- a. **IP address:** An Internet protocol address (or simply “IP address”) is a unique numeric address used by a computer on the Internet. An IP address looks like a series of four numbers, each in the range 0 - 255, separated by periods (e.g., 18.55.7.216). Every computer attached to the Internet must be assigned an IP address so the Internet traffic sent from and directed to that computer may be directed properly from the source to its destination. Most Internet service providers control a range of IP Addresses. The Massachusetts Institute of Technology (“MIT”) controls all IP Addresses which begin with the number 18. Some computers have static – that is, long term – IP addresses, while others have dynamic – that is flexibly assigned or frequently changed – IP addresses.
- b. **MAC address:** A Media Access Control address is a unique identifier assigned to a network interface, in this case, a computer’s network interface card. The MAC address most often is assigned by the manufacturer of the network interface card. Although intended to be a permanent and globally unique identification, it is often possible to change the MAC address on hardware, an action often referred to as “MAC address spoofing.”

**PROBABLE CAUSE**

6. Based on the facts set forth below, there is probable cause to believe that Aaron Swartz:

- a. broke into a network interface closet at the Massachusetts Institute of Technology ("MIT");
- b. without authorization, accessed MIT's computer network from a network switch within that closet;
- c. fraudulently used the appearance of being a MIT student, faculty member or researcher to access JSTOR's extensive electronic library; and
- d. fraudulently took from that library over a million journal articles which JSTOR made available by paid subscription or individual purchase.

**JSTOR**

7. JSTOR, founded in 1995, is a United States-based, on-line system for archiving and providing access to academic journals. It provides full-text searchable digitized copies of over 1,000 academic journals, dating back for lengthy periods of time. JSTOR is an independent, self-sustaining, non-profit organization.

8. It can be extraordinarily expensive, in terms of both cost and space, for a research or university library to maintain a comprehensive collection of academic journals. By digitizing extensive, historical collections of journal titles, JSTOR enables libraries to out-source the storage of these journals, ensures their preservation, and enables authorized users to conduct full-text, cross-disciplinary searches of them.

9. JSTOR licenses all content under copyright from rights holders and gets permission from them both to digitize the content and make the content available online.<sup>1</sup>

10. In the vast majority of instances, JSTOR charges subscription fees to the libraries, universities and publishers who wish to have access to JSTOR's digitized journals. In the

---

<sup>1</sup> Some materials available on JSTOR are not subject to copyright.

instance of a large research university, this annual subscription fee for the various collections of content offered by JSTOR can cost more than fifty thousand dollars. Portions of the subscription fees are shared with the journal publishers who hold the original copyrights. In addition, JSTOR makes available some articles through its Publisher Sales Service, a program offered through participating JSTOR publishers in which journal articles are available for individual purchase. Publishers decide which articles can be purchased and set fees for their articles. JSTOR facilitates the purchase of articles from the archives on behalf of the participating publishers.

#### The Fraudulent Downloads

11. MIT offers short-term service on its computer network to registered campus guests. On September 24, 2010, an individual registered on the network using the pseudonym “Gary Host” and providing the throwaway e-mail address, [ghost@mailinator.com](mailto:ghost@mailinator.com).<sup>2</sup> As part of the registration process, his computer identified the MAC address of its network interface as 00235a735ffb and its client name<sup>3</sup> as “ghost laptop”.

12. On September 25, 2010, shortly after midnight, the “ghost laptop” was assigned IP address 18.55.6.215. Later that day, JSTOR experienced an extraordinary volume of automated requests and downloads from its digitized journal collections to that IP address. The downloads continued into the evening, when JSTOR blocked access to its network from 18.55.6.215.

13. The next morning, JSTOR began to experience rapid and voluminous downloads from IP address 18.55.6.216. Accesses from this address continued until the middle of the day, when JSTOR blocked this IP address as well. That day, JSTOR turned to blocking a much

---

<sup>2</sup> Mailinator is a free disposable e-mail address service that allows a user to create a new e-mail address on the fly. Mailinator will accept mail for any mail address within the mailinator.com domain, and allows anyone to read it without having to create an account or enter a password. All mail sent to mailinator.com is automatically deleted after several hours whether read or not. It is intended to provide users with an anonymous and temporary e-mail address. See <http://mailinator.com/faq.jsp> (Mailinator FAQs), last visited on February 1, 2011.

<sup>3</sup> A computer’s name helps to identify it on a network and can be chosen by a user.



broader range of IP address, temporarily denying service to legitimate JSTOR users at MIT.

14. MIT controls the assignment of all IP addresses in which the first block is “18.” It has assigned the second block in the IP address for use by specific buildings on campus. In this instance, “18.55” defines connections made to the MIT network from within Building 16 on campus.

15. On September 27, 2010, MIT deactivated the guest registration for the “ghost laptop” by barring the MAC address 00235a735ffb from being assigned a new IP address.

16. On October 2, 2010, “Gary Host,” again using a computer with the client name “ghost laptop,” registered as a guest and obtained an IP address from the MIT network. He appears to have bypassed the affirmative bar which MIT had placed to his usage of the network by spoofing the MAC Address of the “ghost laptop,” changing the last byte of the MAC address from 00235a735ffb to 00235a735ffc (changing the final “b” to “c”). The “ghost laptop” was assigned IP address 18.55.7.48.

17. On October 8, 2010, the perpetrator, using the same naming conventions as he had for “ghost laptop,” obtained a guest registration simultaneously for a second computer on the MIT network. “Grace Host” registered the computer client “ghost macbook,” providing the e-mail address [ghost42@mailinator.com](mailto:ghost42@mailinator.com).<sup>4</sup> The MIT network assigned the “ghost macbook” IP address 18.55.5.100, locating the “ghost macbook’s” network connection somewhere within Building 16.

18. Extraordinary downloading of JSTOR’s digitized copies of journals began just before 3:00 p.m. on October 9, 2010, from IP address 18.55.5.100 (assigned to the “ghost macbook”) and continued until approximately 7:00 p.m. In parallel, extraordinary downloading from JSTOR’s collections to IP address 18.55.7.48 (assigned to the “ghost laptop”) began at approximately 6:30 p.m. and continued as well until approximately 7:00 p.m. that night.

---

<sup>4</sup> The MAC address of the “ghost macbook,” 0017f22cb074,” is within the range coded by Apple into hardware it manufactures.

19. During the months of November and December, 2010, over two million illegal downloads were made from JSTOR to two IP addresses assigned to Building 16 at MIT; 18.55.6.240 and 18.55.7.240. Of these, approximately half were research articles, with the remainder being reviews, news, editorials, and miscellaneous things. This is more than one hundred times the number of downloads by all the legitimate MIT JSTOR users combined during the same period.

20. JSTOR did not spot this phase of illegal downloading until Christmas time. MIT's network logs reflect that the computer assigned IP address 18.55.6.240 had not registered as a guest on the MIT computer network on this occasion. An analysis on January 4, 2011, however, reflected that both IP addresses 18.55.6.240 and 18.55.7.240 were assigned to a computer with the MAC address 004ce5a0c756. Using network tools available to MIT on this occasion, the computer was tracked back to a specialized network wiring closet in the basement of Building 16 at MIT.

21. There, MIT personnel found, and subsequently showed to law enforcement personnel, the ACER LAPTOP and an external Samsung hard drive, both of which had been concealed under a cardboard box. The laptop had been connected directly into MIT's computer network and the perpetrator had assigned to himself the IP addresses 18.55.6.240 and 18.55.7.240.

22. On January 4, 2011, MIT placed a video camera in the wiring closet. Later that day, the perpetrator, subsequently identified as Aaron Swartz, was videotaped entering the wiring closet. While there, he appeared to replace the external hard drive attached to the laptop.

23. Swartz, who is neither a student nor an employee of MIT, was recorded again entering the wiring closet on January 6, 2011. Before law enforcement officers could get there, he had removed his computer equipment from the closet and left.

24. Later, during the afternoon of January 6, 2011, the laptop removed from the network wiring closet (identified by its MAC address 004ce5a0c756) was plugged into a network



jack in Building W20. There, it was once again registered through MIT's guest services. When it was, the computer identified itself as "ghost laptop," the same identification provided during the illegal downloads in September and October. The ACER LAPTOP and the WESTERN DIGITAL HARD DRIVE were located and recovered by MIT personnel and law enforcement, without the previously observed external hard drive.

25. An MIT police officer who had seen several pictures taken by the covert camera in Building 16's network wiring closet saw Aaron Swartz on a bicycle near MIT, approximately half an hour after the "ghost laptop" had been connected in Building W20. The officer stopped his car, activated its blue lights and displayed his wallet badge. When he sought to question Swartz, Swartz dropped his bike to the ground<sup>5</sup> and fled. The backpack in Swartz's possession at the time he was caught and arrested minutes later appeared to be the same one he had with him on each occasion he was videotaped in the wiring closet at MIT.

26. In the backpack was the USB DRIVE. From my training and experience and information provided to me by other agents, USB drives are frequently used to store software applications, data and records, including .pdf formatted records such as those that were illegally downloaded from JSTOR. They are also frequently used to transfer records and data between computers or hard drives, such as between those connected in the wiring closet to MIT's network and ones available to Swartz outside.<sup>6</sup>

27. On February 9, 2011, the Court issued warrants to search Swartz's residence at 950 Massachusetts Avenue, Apartment 320, Cambridge, Massachusetts 02139 ("the PREMISES"), the ACER LAPTOP, the WESTERN DIGITAL HARD DRIVE, and the USB

---

<sup>5</sup> I mistakenly stated in my February 9<sup>th</sup> Affidavit that Swartz dropped his backpack to the ground before fleeing from police. He kept it with him when he fled.

<sup>6</sup> As reflected in paragraphs 17 and 18, above, there were two laptops used in the October 9, 2010, illegal downloads from JSTOR. One identified itself to MIT's network as "ghost laptop." The second identified itself to the MIT's network as "ghost macbook" and provided a MAC address within the range coded by Apple into hardware it manufactures. The "ghost macbook" used in the fraud and thefts has not been recovered yet.

DRIVE. The warrant to search the PREMISES was executed on February 11, 2011. The warrants to search the ACER LAPTOP, the WESTERN DIGITAL DRIVE, and the USB DRIVE were not executed prior to their expiration on February 22, 2011. At the time the warrant was issued for these pieces of electronic equipment, they were secured within the Identification Unit Laboratory of the Cambridge Police Department. Throughout the period of February 9, 2011, to the present, they remained within secure areas at Cambridge Police Headquarters, first in the Identification Unit Laboratory, then in the Evidence/Property Unit.

28. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or even years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

- a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.
- b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual

memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

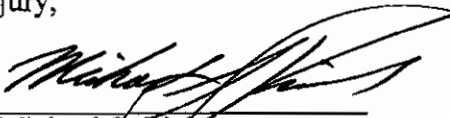
d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

### CONCLUSION

29. Based on the information described above, I have probable cause to believe that Aaron Swartz has violated 18 U.S.C. § 1030(a)(2) (intentionally accessing a computer without authorization and obtaining information with a value that exceeds \$5,000), 18 U.S.C. § 1030(a)(5)(A) (intentionally causing damage without authorization to a protected computer) and 18 U.S.C. § 1343 (wire fraud).

30. Based on the information described above, I also have probable cause to believe that evidence, fruits, and instrumentalities of these crimes, as described in Attachment B, are contained within the ACER LAPTOP, the WESTERN DIGITAL HARD DRIVE and the USB DRIVE.

Sworn to under the pains and penalties of perjury,

  
Michael S. Pickett  
Special Agent  
United States Secret Service

Subscribed and sworn to before me on February 24, 2011

  
CHIEF UNITED STATES MAGISTRATE JUDGE



**ATTACHMENT A**

**PREMISES TO BE SEARCHED**

Acer Aspire One laptop computer, serial number LUSAX0D001001100E1601

2.0 terabyte Western Digital hard drive, serial number WMAZA1626675

HP USB drive, marked 0045SMKBT1 85102

**ATTACHMENT B**

**ITEMS TO BE SEIZED**

- I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1030(a)(2) (intentionally accessing a computer without authorization and obtaining information with a value that exceeds \$5,000), 18 U.S.C. § 1030(a)(5)(A) (intentionally causing damage without authorization to a protected computer) and 18 U.S.C. § 1343 (wire fraud), including, without limitation:
  - A. Records and tangible objects pertaining to the following entities, websites, computer networks, and IP addresses:
    - 1. JSTOR
    - 2. Massachusetts Institute of Technology
    - 3. Jstor.org
    - 4. Mit.edu
    - 5. IP addresses in the class A domain 18.
  - B. Records and tangible objects pertaining to the following topics:
    - 1. JSTOR
    - 2. Records and data digitized by JSTOR, including, without limitation, journals digitized by JSTOR
    - 3. Records and data stored on JSTOR
    - 4. Records and data originating on JSTOR
    - 5. Means of access to JSTOR
    - 6. Computer software capable of making repeated requests for data and records from JSTOR
    - 7. Computer software capable of making repeated downloads of records and data from JSTOR

8. MIT's computer network
  9. MIT's physical plant
  10. Remote electronic storage locations
  11. MAC addresses
- C. Records and tangible objects pertaining to the existence and identity of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the crimes listed above;
- D. Records and tangible objects pertaining to communications to any third parties in anticipation, during or following the crimes listed above about those crimes;
- E. Records and tangible objects relating to the ownership, occupancy, or use of 950 Massachusetts Avenue, Apartment 320, Cambridge, Massachusetts 02139 and assigned storage locker "C4", Acer Aspire One laptop computer, serial number LUSAX0D001001100E1601, 2.0 terabyte Western Digital hard drive, serial number WMAZA1626675, and HP USB drive, marked 0045SMKBT1 85102; and
- F. For any computer hardware, computer software, computer-related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):
1. evidence of who used, owned, or controlled the computer equipment;
  2. evidence of computer software that would allow remote access and control of the computer equipment
  3. evidence of the attachment of other computer hardware or storage



- media;
- 4. evidence of counter-forensic programs and associated data that are designed to eliminate data;
- 5. evidence of the times the computer equipment was used;
- 6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment; and
- 7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media.

- II. All computer hardware, computer software, computer-related documentation, and storage media. Off-site searching of these items shall be limited to searching for the items described in paragraph I.

#### **DEFINITIONS**

For the purpose of this warrant:

- A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.
- B. "Computer hardware" means any electronic device capable of data processing (such as a computer, personal digital assistant, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
- C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility,



communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

- D. "Computer-related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
- E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).
- F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.
- G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

**Attachment A**

HP USB drive, marked 0045SMKBT1 85102

**ATTACHMENT B**

**ITEMS TO BE SEIZED**

- I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1030(a)(2) (intentionally accessing a computer without authorization and obtaining information with a value that exceeds \$5,000), 18 U.S.C. §1030(a)(5)(A) (intentionally causing damage without authorization to a protected computer) and 18 U.S.C. § 1343 (wire fraud), including, without limitation:
  - A. Records and tangible objects pertaining to the following entities, websites, computer networks, and IP addresses:
    1. JSTOR
    2. Massachusetts Institute of Technology
    3. Jstor.org
    4. Mit.edu
    5. IP addresses in the class A domain 18.
  - B. Records and tangible objects pertaining to the following topics:
    1. JSTOR
    2. Records and data digitized by JSTOR, including, without limitation, journals digitized by JSTOR
    3. Records and data stored on JSTOR
    4. Records and data originating on JSTOR
    5. Means of access to JSTOR
    6. Computer software capable of making repeated requests for data and records from JSTOR
    7. Computer software capable of making repeated downloads of records and data from JSTOR

8. MIT's computer network
  9. MIT's physical plant
  10. Remote electronic storage locations
  11. MAC addresses
- C. Records and tangible objects pertaining to the existence and identity of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the crimes listed above;
- D. Records and tangible objects pertaining to communications to any third parties in anticipation, during or following the crimes listed above about those crimes;
- E. Records and tangible objects relating to the ownership, occupancy, or use of 950 Massachusetts Avenue, Apartment 320, Cambridge, Massachusetts 02139 and assigned storage locker "C4", Acer Aspire One laptop computer, serial number LUSAX0D001001100E1601, 2.0 terabyte Western Digital hard drive, serial number WMAZA1626675, and HP USB drive, marked 0045SMKBT1 85102; and
- F. For any computer hardware, computer software, computer-related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):
1. evidence of who used, owned, or controlled the computer equipment;
  2. evidence of computer software that would allow remote access and control of the computer equipment
  3. evidence of the attachment of other computer hardware or storage

- media;
  - 4. evidence of counter-forensic programs and associated data that are designed to eliminate data;
  - 5. evidence of the times the computer equipment was used;
  - 6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment; and
  - 7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media.
- II. All computer hardware, computer software, computer-related documentation, and storage media. Off-site searching of these items shall be limited to searching for the items described in paragraph I.

#### **DEFINITIONS**

For the purpose of this warrant:

- A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.
- B. "Computer hardware" means any electronic device capable of data processing (such as a computer, personal digital assistant, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
- C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility,

communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

- D. "Computer-related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
- E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).
- F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.
- G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

OLD

## 13.0 Information Policies

### 13.2 Policy on the Use of Information Technology

---

Information technology policies ensure that everyone's use of the Institute's computing and telecommunications resources supports its educational, research, and administrative mission in the best possible way. Effective support of the Institute's mission requires complying with relevant legal, contractual, professional, and policy obligations whenever information technology is used. Effective support also means that individuals should not interfere with the appropriate uses of information technology by others.

This policy statement covers privacy of Institute records; information security and preservation; responsible use of MIT computers, networks, and telephones; privacy of electronic communications; and the acquisition and use of third-party products and services.

#### 13.2.1 Privacy of Institute Records

All members of the MIT community are responsible for ensuring that their handling of information about individuals is consistent with the Institute's policy on privacy of information (see [Section 11.2](#)). This policy applies to all records of the Institute and to any other appearances of all or part of the information in those records.

The privacy of individuals must be protected, regardless of the form or the location in which the information about them is stored, including computer media. Access to personal information must be limited to authorized users for approved purposes. Such information must be safeguarded from unauthorized access. Individuals who are authorized to access personal information about others should not make unauthorized disclosure or use of it.

The availability of computerized information about individuals may appear to encourage the use of those records for purposes beyond those for which the information was originally collected. Such secondary uses of information about individuals are inappropriate, unless undertaken in accordance with the Institute's policy on privacy.

#### 13.2.2 Information Security and Preservation

MIT has an obligation to provide accurate, reliable information to authorized recipients and to preserve vital records (see [Section 13.3 Archival Policy](#)). MIT is increasingly dependent on the accuracy, availability, and accessibility of information stored electronically and on the computing and networking resources that store, process, and transmit this information. Records created and maintained in electronic form are included in the Institute's definition of archival materials.

Individuals who manage or use the information and computing resources required by the Institute to carry out its mission must protect them from unauthorized modification, disclosure, and destruction. Information — including data and software — is to be protected, regardless of the form or medium that carries the information. Protection shall be commensurate with the risk of exposure and with the value of the information and of the computing resources.

#### 13.2.3 Responsible Use of MIT Computers, Networks, and Telephones

MIT's computers, networks, and telephones offer many opportunities to share information on campus and



to access resources off campus. All members of the MIT community are obligated to use these facilities in accordance with applicable laws, with Institute standards of honesty and personal conduct, and in ways that are responsible, ethical, and professional.

The use of MIT's telephones is restricted to Institute business and necessary personal telephone calls. Necessary personal telephone calls include calls to arrange family and personal schedules, medical-related calls, and other reasonable calls; these calls should be brief. No reimbursement to MIT is required for such calls.

Telephone calls related to personal businesses and activities are prohibited unless a personal telephone credit card is used or an explicit agreement for reimbursement to MIT has been established with the appropriate organization.

MIT's computing and networking facilities and services are to be used for Institute purposes only and not for the benefit of private individuals or other organizations without authorization. Unauthorized access to and use of MIT computer and network services violates this policy.

Members of the Institute community should not take unauthorized actions to interfere with or alter the integrity of MIT computers, networks, telephones, or the information accessed through them. Efforts to restrict or deny access by legitimate users of the Institute's computers, networks, and telephones are unacceptable. Individuals should not use MIT facilities to interfere with or alter the integrity of any other computers, networks, telephones, or information, irrespective of their location.

Destruction, alteration, or disclosure of data or programs belonging to others without authorization is inappropriate. Individuals should not connect unauthorized equipment to or tamper with MIT information technology facilities or equipment. Using any of the information technology resources of the Institute for unethical purposes, such as harassment, is unacceptable.

#### 13.2.4 Privacy of Electronic Communications

Federal laws protect the privacy of users of wire and electronic communications from illegal interception. Individuals who access electronic files or intercept network communications at MIT or elsewhere without appropriate authorization violate Institute policy and may be subject to criminal penalties.

The law also regulates disclosure of information within an electronic mail system by providers of electronic mail services. MIT departments and other providers of electronic mail services at the Institute who are asked to disclose information from an individual's electronic files without the individual's authorization should seek guidance from the Office of the Vice President for Information Systems.

#### 13.2.5 Acquisition and Use of Third-Party Products and Services

Special restrictions are often placed on the use of information technology products and services — such as hardware, software, documentation, and databases — acquired from outside sources. Members of the MIT community are required to abide by the restrictions imposed by suppliers on information technology products and services acquired for use at the Institute.

Unless it has been placed in the public domain, most third-party software is protected by copyright law. Under US copyright law, it is illegal to duplicate copyrighted software or documentation — except for one archival copy — without the permission of the copyright owner. Unauthorized copying includes lending software to others so that they can make unauthorized copies, as well as letting someone use your computer to make an unauthorized copy. It is illegal to distribute unauthorized copies of software by any means, including a computer network.

Use of hardware, software, databases, and documentation may be further restricted by patent law, as a trade secret, or by contract law in the form of a license or other agreement. When a department, laboratory, center, or individual acquires hardware, software, documentation, or access to proprietary databases from outside sources for use at MIT, the department is responsible for obtaining Institute approval that the terms and conditions of any associated license or other agreement are consistent with relevant Institute policy, such as the research policy statements and the policies on Intellectual Property (see Section 13.1).

When supervisors, instructors, or others arrange for authorized distribution of information technology products and services from outside sources, those individuals are responsible for ensuring that the people having access to the products and services are advised of all the associated usage restrictions.

**UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS**

<b>UNITED STATES OF AMERICA</b>	)	
	)	
v.	)	<b>Criminal No. 11-10260-NMG</b>
	)	
<b>AARON SWARTZ,</b>	)	
	)	
<b>Defendant</b>	)	

**GOVERNMENT’S RESPONSE TO  
MOTION TO DISMISS COUNTS 1 AND 2**

Defendant Swartz has moved to dismiss Counts 1 and 2 of the Superseding Indictment, which charge him with committing wire fraud. He argues that a communication between two computers cannot constitute wire fraud; that, as a matter of law, he could not have acted in a materially deceptive way with respect to either MIT or JSTOR; and, finally, that the wire fraud statute would be void for vagueness as applied to his case.

The Court should deny Swartz’s motion to dismiss. The Superseding Indictment alleges a scheme to defraud JSTOR of its property through interstate wire communications. The wire fraud statute has been applied for decades in analogous situations. Consequently, Swartz had fair notice that his contemplated conduct was forbidden by the statute and the wire fraud statute is not void for vagueness as applied to his conduct.

**I. THE SUPERSEDING INDICTMENT ADEQUATELY ALLEGES A SCHEME TO DEFRAUD**

Swartz’s motion to dismiss should be denied because the Superseding Indictment adequately alleges the elements of a wire fraud crime and conduct that is prohibited by that statute. “In the normal course of events, a facially valid indictment returned by a duly constituted grand jury calls for a trial on the merits. An indictment is generally sufficient if it

sketches out the elements of the crime and the nature of the charge so that the defendant can prepare a defense and plead double jeopardy in any future prosecution for the same offense.”

*United States v. George*, 839 F. Supp. 2d 430, 434-35 (D. Mass. 2012) (Gorton, D.J.) (citations and internal quotation marks omitted). Thus, to prevail on a motion to dismiss, Swartz must show that the conduct charged in the Superseding Indictment is not prohibited by the language of the statute. *United States v. Pirro*, 212 F.3d 86, 91 (2d Cir. 2000) (affirming dismissal of a tax count that failed to charge a violation of a known legal duty).

The elements of wire fraud are: (1) a scheme to defraud or obtain money or property by means of false or fraudulent pretenses, involving a material misrepresentation; (2) the defendant’s knowing and willful participation in the scheme with the intent to defraud; and (3) the use of interstate wire communications in furtherance of the scheme. *First Cir. Pattern Jury Instr. (Criminal)* 4.13 (1998); *Neder v. United States*, 527 U.S. 1, 25 (1999). The Superseding Indictment alleges each of these elements explicitly. Paragraph 35 charges that Swartz “having devised and intended to devise a scheme and artifice to defraud and for obtaining property — journal articles digitized and distributed by JSTOR, and copies of them — by means of material false and fraudulent pretenses and representations, transmitted and caused to be transmitted by means of wire communication in interstate commerce writings, signs, and signals — that is, communications to and from JSTOR’s computer servers — for the purpose of executing the scheme, and aiding and abetting it, including on or about” dates specified in that paragraph. Superseding Indictment ¶ 35. Categorized by elements of the offense, these allegations thus allege (1) a scheme to defraud or obtain JSTOR’s property by means of false or fraudulent pretenses, involving a material misrepresentation; (2) Swartz’s knowing and willful participation

in the scheme with the intent to defraud; and (3) the use of interstate wire communications in furtherance of the scheme. *See First Cir. Pattern Jury Instr. (Criminal)* 4.13 (1998); *Neder*, 527 U.S. at 25.

Swartz's wire fraud scheme is fleshed out in other paragraphs of the Superseding Indictment. Paragraphs 34 (a)-(d) identify fraudulent pretenses and misrepresentations through which Swartz obtained JSTOR's journal articles, specifically:

- a. Deceptively making it appear to JSTOR that he was affiliated with MIT by downloading JSTOR's articles through MIT's computer network and from MIT IP addresses, even though he was not affiliated at the time with MIT, Superseding Indictment ¶ 34(a);
- b. Repeatedly taking steps to change his and his computer's apparent identities and to conceal his and his computer's true identities, Superseding Indictment ¶ 34(b);
- c. Using a rapid, automated software tool designed to make it appear as if he were multiple people making single download requests rather than a single person making multiple requests, Superseding Indictment ¶ 34(c); and
- d. Attempting to conceal from MIT the physical location of his laptop's connection to MIT's network, by placing it in a wiring closet, covering it with cardboard, and, at one point, moving it from one MIT building to another, Superseding Indictment ¶ 34(d).

A number of paragraphs in the Superseding Indictment demonstrate how those fraudulent pretenses and misrepresentations were material. They explain that by changing his computers' IP addresses, Swartz sought to mislead JSTOR, and misled JSTOR, which could identify and attempt to block the source of the exhaustive download requests it was suffering only by the IP address from which the download requests were coming. Superseding Indictment ¶¶ 17(a)-(c), 19(c), 24, 27(b). By changing his computers' MAC addresses, Swartz similarly sought to mislead MIT, and misled MIT, which could only identify him and block his access to their network by barring the MAC address of his computer from being used during the "guest"

registration process. Superseding Indictment ¶¶ 17(d), 19(b), 27(c). By using software designed to make it appear as if his computer was multiple computers or people making single download requests rather than a single person making multiple download requests, Swartz sought to deceive JSTOR, and deceived JSTOR, which limited the number of articles that any one person could download. Superseding Indictment ¶¶ 28, 34(c). By placing his computer under a cardboard box, Swartz sought to deceive MIT personnel into not noticing or disconnecting the computer. *See* Superseding Indictment ¶¶ 24, 34(d). By moving it from one part of MIT's campus to another, Swartz sought to evade detection. Superseding Indictment ¶¶ 27, 34(d). Throughout, Swartz did not use his real name when he registered his computer, thus seeking to avoid and avoiding MIT's and JSTOR's attempts to verify his actual identity. Superseding Indictment ¶¶ 14(a), 19(a), 20, 27(a), 34(b).<sup>1</sup>

The Superseding Indictment's allegations far more than met the pleading standards.

Swartz argues generally that none of these false and fraudulent pretenses or misrepresentations were material, as the wire fraud statute requires. This is for the jury to decide. *See United States v. Senibaldi*, 959 F.2d 1131, 1133 (1st Cir. 1992) (holding that on a motion to dismiss an indictment, the court should resolve questions of pleading, not evidence); *United States v. Guerrier*, 669 F.3d 1, 3-4 (1st Cir. 2011) ("And his attempt to sink a facially valid indictment with a motion to dismiss that targets the strength of the government's *evidence* misfires. [¶] What counts in situations like this are the charging paper's *allegations*, which we

---

<sup>1</sup> Swartz argues at the bottom of page 7 and top of page 8 of his motion that misrepresentations made to MIT cannot support a charge of defrauding JSTOR of JSTOR's property. The First Circuit has expressly rejected this "convergence theory." "Nothing in the mail and wire fraud statutes requires that the party deprived of money or property be the same party who is actually deceived." *United States v. Christopher*, 142 F.3d 46, 54 (1st Cir. 1998).

must assume are true. Consistent with that rule, courts routinely rebuff efforts to use a motion to dismiss as a way to test the sufficiency of the evidence behind an indictment's allegations . . . .") (citations omitted).

Swartz more particularly argues that his fraudulent pretenses and misrepresentations were not material because he made them not to a person but to a computer, arguing that a computer is not a "decisionmaker" and therefore a pretense or misrepresentation made to a computer cannot be material. This argument, too, fails on a number of fronts. First, the argument rests on Swartz's presumption that the Government lacks evidence that his pretenses and misrepresentations were considered by a human, whereas a motion to dismiss should consider only the indictment's allegations, not the evidence. *See Guerrier*, 669 F.3d at 3-4; *Senibaldi*, 959 F.2d at 1133. (In fact, to the extent that it is relevant, the Government anticipates introducing testimony that some of Swartz's pretenses and misrepresentations were reviewed by humans: MIT's and JSTOR's network security personnel.) Second, Swartz's presumption that none of his pretenses and misrepresentations were considered by a decisionmaker is belied by the Superseding Indictment's allegations that MIT and JSTOR responded to Swartz's pretenses and misrepresentations by blocking his access and downloads or were sometimes misled into failing to block his access and downloads. Third, whether Swartz's pretenses and misrepresentations went to a computer rather than a person is beside the point. The gravamen of the wire fraud offense is to "transmit[] or cause[] to be transmitted by means of wire . . . communications . . . writings, signs, signals, pictures, or sounds . . ." 18 U.S.C. § 1343. Representations transmitted by wire are necessarily transmitted from one electronic device to another electronic device. This is how telephone calls, electronic mail, and the Internet work.



To suggest that the wire fraud statute excludes communications that are received by an electronic device would be to severely restrict the statute's reach in ways not contemplated by the statute's language or by any court. Fourth, even when Swartz's pretenses and misrepresentations were not reviewed specifically by a person, they were nevertheless considered by MIT and JSTOR for purposes of deciding whether to block or allow Swartz's access and downloads. Those decisions might have been made by computers, but those computers had been programmed by humans to automate MIT's and JSTOR's security decisions. When Swartz misled their computers about his and his computers' identity to access their networks, he made material representations to MIT and JSTOR every bit as much as if he had provided false identification to deceive guards at their doors to access their buildings.<sup>2</sup>

In fact, as Defendant is aware, the wire fraud statute has been repeatedly used to charge defendants for transmitting deceptive communications from one electronic device to another electronic device to trick the victim into providing electronic service. *See, e.g., United States v. Harris*, 2012 WL 2402788 (D. Mass. 2012) (Wolf, C.J.) (denying motion to dismiss or for acquittal of wire fraud conviction for selling cable modem hacking software that would allow users to obtain free Internet service by mimicking identities, including MAC addresses, used by Internet service providers to identify legitimate subscribers); *United States v. Manzer*, 69 F.3d 222 (8th Cir. 1995) (upholding mail and wire fraud convictions against defendant who modified satellite broadcast decryption devices to allow customers to watch premium television channels such as HBO for free) (discussed in *Harris, supra*); *United States v. Coyle*, 943 F.2d 424 (4th

---

<sup>2</sup> In an analogous context, tax fraud is no less tax fraud just because the IRS has recently computerized its tax return submission and review process.

Cir. 1991) (mail fraud conviction for defendant who built and sold cable and television descramblers to allow nonsubscribers free cable service); *United States v. Gautreaux*, 382 F.2d 607, 610 (10th Cir. 1967) (upholding wire fraud conviction for scheme to defraud telephone company of revenue for use of long distance services; declaring that financial loss to telephone company or gain to defendants was unnecessary); *United States v. Patterson*, 528 F.2d 1037 (5th Cir. 1976) (holding that since defendant knew “blue boxes” were intended to defraud telephone company of revenue from long distance calls, he could not successfully argue that he had not received fair notice that wire fraud statute applied); *United States v. DeLeeuw*, 368 F. Supp. 426 (E.D. Wisc. 1974) (upholding application of wire fraud statute to schemes to obtain free telephone service).<sup>3</sup>

Not all theft is, of course, mail or wire fraud. But when the conduct involves repeated deception and deceit, as Swartz’s conduct did, the wire fraud statute encompasses the crime. *U.S. v. Coyle*, 943 F.3d at 427 (distinguishing fraud, which is characterized “trick, deceit, chicane and overreaching” and by “dishonest methods or schemes,” from deprivation of property by such crimes as “theft by violence.. robbery and burglary”) (citations omitted). The Superseding Indictment properly alleges a wire fraud and therefore should not be dismissed.

---

<sup>3</sup> With the exception of *Harris*, these cases were decided before *Neder*, in which the Supreme Court made clear that a material misstatement was a necessary element of a wire fraud charge. They are cited here only to show that numerous district and appellate courts have upheld the application of the wire fraud statute in similar contexts.

## II. THE COMPUTER FRAUD STATUTE DID NOT PREEMPT OR REPEAL THE WIRE FRAUD STATUTE'S APPLICATION TO COMPUTER-TO-COMPUTER WIRE COMMUNICATIONS

Swartz suggests, without citation either to legislative history or caselaw, that when Congress enacted the Computer Fraud and Abuse Act provisions in 18 U.S.C. § 1030(a)(2) (obtaining information from a computer) and (a)(4) (using a computer to defraud), Congress expressed its belief that criminal conduct such as Swartz's was not covered by the wire fraud statute.

Neither the Computer Fraud and Abuse Act nor the wire fraud statute expressly preempts the other. That leaves Swartz to argue that the Computer Fraud and Abuse Act repealed or preempted the wire fraud statute by implication.

This contradicts the normal rules of statutory interpretation. By making this argument, Swartz ignores First Circuit precedent discouraging the interpretation of one criminal statute to preclude charging a defendant under another criminal statute:

Assuming, arguendo, that appellants' acts violated both 7 U.S.C. § 60 and 18 U.S.C. § 1341 or 1343, we find no basis that the former either preempted or impliedly repealed the latter. . . .

Moreover, in urging a finding of implied repeal, appellants march into the teeth of a strong judicial policy disfavoring the implied repeal of statutes. For a court to find implied repeal, there must be a positive repugnancy between the two statutes. Where two statutes cover the same subject, effect will be given to both, if possible. Partial repeals will not be implied because they do not satisfy the requirement that the intent of the legislative body be clear and unequivocal. It is also generally held that for a later-enacted statute to impliedly repeal an earlier one, the later statute must cover the entire field occupied by the earlier one. . . .

Although the [commodities fraud and mail and wire fraud] statutes prohibit similar conduct, they operate independently and harmoniously. The government's election to prosecute appellants

under the statute which, at the time, provided the more severe penalty, was an exercise of discretion that violated no rights of appellants.

*United States v. Brien*, 617 F.2d 299, 310-11 (1st Cir. 1980) (citations and footnote omitted).

Consequently, the First Circuit held that the anti-fraud provisions of the Commodities Futures Trading Act did not impliedly preempt the wire fraud statute's coverage of the same criminal conduct. *Id.*

Swartz's argument for the Computer Fraud and Abuse Act's implied repeal or preclusion of the wire fraud statute is similarly doomed. Under *Brien*, there is "a strong judicial policy disfavoring the implied repeal of statutes," such that "[w]here two statutes cover the same subject, effect will be given to both, if possible." *Id.* at 310. Since the Computer Fraud and Abuse Act and the wire fraud statute cover the same subject, "effect will be given to both, if possible." *Id.* Moreover, "for a later-enacted statute" like the Computer Fraud and Abuse Act "to impliedly repeal an earlier one, the later statute must cover the entire field occupied by the earlier one," *id.*, yet the Computer Fraud and Abuse Act does not cover every type of wire communication covered by the wire fraud statute. Furthermore, "[a]lthough the [Computer Fraud and Abuse Act and the wire fraud] statutes prohibit similar conduct, they operate independently and harmoniously." *Id.*

In fact, numerous cases have held that a defendant's criminal conduct could be prosecuted under the wire or mail fraud statute and a more specific criminal statute. *See, e.g., United States v. Coyle*, 943 F.2d 424, 427 (4th Cir. 1991) (holding that defendant who built and sold cable and television descramblers to allow nonsubscribers free cable service could be charged with either mail fraud or statute specific to cable communications, stating that "[i]t is of

no consequence that [the defendant] could have been prosecuted under § 553. The possibility of such a prosecution does not preclude the United States Attorney from electing to charge violation of the mail fraud statute.”); *United States v. Faulhaber*, 929 F.2d 16, 19 (1st Cir.1991) (upholding application of § 1341 and securities fraud statute to the same conduct); *United States v. Brien*, 617 F. 2d 299, 309-10 (1st Cir. 1980) (§ 1341 and anti-fraud provisions of Commodities Futures Trading Act).

More specifically, the Eleventh Circuit has recognized that 18 U.S.C. §§ 1030(a)(2), (a)(4) and 1343 can be charged together against the same fraudulent conduct. *Cf. United States v. Barrington*, 643 F.3d 1178, 1191 (11th Cir. 2011) (“We have no hesitation in concluding that the Government’s theory rested on a legally cognizable theory of conspiracy to defraud by wire and computer, through which the conspirators deprived [the victim] of its property interest”).

Consequently, Swartz has no grounds to claim that the wire fraud statute does not cover computer-to-computer communications.

### **III. THE WIRE FRAUD STATUTE IS NOT VOID FOR VAGUENESS AS APPLIED TO SWARTZ**

Swartz finally argues that the wire fraud statute as applied to his conduct would be void for vagueness. He had, he says, no warning that his conduct was wrongful.

As a factual matter, this argument is incredible. Swartz took great pains to hide his identity, to hide his laptop and its identifiers, and to hide his face by a bicycle helmet when he believed he could be seen leaving and entering the closet. *See* Superseding Indictment ¶¶ 17, 19, 20, 24, 26, 27, 28, 34. These allegations demonstrate Swartz’s consciousness of guilt, not blithe ignorance of criminality.

Moreover, the wire fraud statute has been used numerous times to charge analogous

behavior. In each instance, as in the present case, the wire fraud statute was applied where:

- (1) no actual or potential human “decisionmaker” heard or would hear the misrepresentation directly;
- (2) the misrepresentation was an electronic one, a claim to a right for services and a deceptive act to avoid paying for them; and
- (3) the deceived company was not deprived of their only copy of something, but rather a service of value for which they charged customers and received payment.

For example, early on, when long-distance telephone service was costly, the wire fraud statute was properly used to convict individuals who sought to defraud the telephone company by using electronic black boxes to deceive their billing computers. *See, e.g., United States v. Gautreaux, supra; United States v. Patterson, supra; United States v. DeLeeuw, supra.* And years later, after technology changed, the wire fraud statute was properly used to convict individuals who used electronic devices to obtain free cable service. *See, e.g., United States v. Manzer*, 69 F.3d 222 (8th Cir. 1995) (mail and wire fraud convictions); *United States v. Coyle, supra* (mail fraud conviction).

For these reasons, Chief Judge Wolf recently rejected a void-for-vagueness challenge to the wire fraud in a similar case that involved using hardware and software to obtain free Internet service. *United States v. Harris, supra.* In *Harris*, the defendant was charged with conspiracy to commit wire fraud and aiding and abetting wire fraud, all for working with a company that developed and sold products to hack cable modems to obtain Internet service without paying for it. 2012 WL 2402788 at \*1. Harris’s conduct shared some similarities with Swartz’s, as Harris’s products helped to hack MAC addresses. *Id.* Harris challenged his conviction on the ground that the wire fraud statute was void for vagueness as applied to his conduct.

Chief Judge Wolf made short work of the challenge. “[T]he Due Process clause of the Fifth Amendment requires that a criminal statute be found unconstitutionally vague if it fails to give a person of ordinary intelligence fair notice that his contemplated conduct is forbidden by the statute.” *Id.* at \*2 (quoting *United States v. Maquardo*, 149 F.3d 36, 41 (1st Cir. 1998)) (alterations omitted). In *Harris*, the “case represent[ed] a straightforward application of the wire fraud statute,” *id.* at \*4, because the wire fraud statute’s scope is broad, the statute “covers deceptive schemes to deprive victims of a wide variety of tangible and intangible property interests,” *id.* (internal quotation marks and citation omitted), and “[t]he plain language of the statute put the defendant on notice that he could be subjected to criminal punishment for devising a scheme to defraud internet service providers, or to obtain money or property from internet service providers by means of false or fraudulent representations, if the scheme involved interstate wire transmissions,” *id.* Chief Judge Wolf then noted that the wire fraud statute had been used numerous times to prosecute similar defendants, such as those who had obtained television or long-distance telephone service without paying for it. *See id.* (citing *Manzer* and other cases).

The same analysis applies to Swartz. As with *Harris*, Swartz’s scheme involved using computer hardware and software, falsifying MAC addresses, and using computer-to-computer communications to obtain service and property without paying for it.<sup>4</sup> The wire fraud statute still

---

<sup>4</sup> Swartz claims that nothing he did deprived MIT or JSTOR of revenue, because he could have used MIT’s and JSTOR’s networks for free. Again, Swartz is not allowed to argue evidence on a motion to dismiss. And his claims contradict the Superseding Indictment’s allegations that MIT offered guests only fourteen days of network use a year, Superseding Indictment ¶ 7, that MIT and JSTOR had blocked his communications repeatedly, *see generally id.*, that Swartz had circumvented JSTOR’s limitations on the number of downloads it permitted, *id.* ¶ 34(c), and that if Swartz had wanted to access JSTOR for legitimate purposes, he could



covers a broad variety of deceptive schemes to deprive victims of a wide variety of tangible and intangible property interests, and the statute's plain language and prior cases still put him on notice that he could be subjected to criminal punishment for devising a scheme to defraud Internet companies by means of false or fraudulent representations, if the scheme involved interstate wire transmissions. That is what the grand jury charged here.

Moreover, if Swartz is convicted, the trial jury will necessarily have found that he acted deliberately and with intent to defraud, which will further contradict his claim that he did not know that his conduct was wrongful. *See id.* at \*5 (noting that finding of deliberate acts with intent to defraud contradicts claim that statute is void for vagueness).

#### IV. CONCLUSION

For these reasons, Swartz's Motion to Dismiss Counts 1 and 2 of the Indictment is without merit and should be denied.

Respectfully submitted,

CARMEN M. ORTIZ  
United States Attorney

By: /s/ Stephen P. Heymann  
STEPHEN P. HEYMANN  
SCOTT L. GARLAND  
Assistant U.S. Attorneys

---

have done so through his JSTOR access at Harvard University's Safra Center for Ethics rather than at MIT, *id.* ¶ 9. On pre-trial motion to dismiss, the Court must accept the indictment's factual allegations as true. *See United States v. Ferris*, 807 F.2d 269, 271 (1st Cir. 1986).

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/s/ Stephen P. Heymann  
STEPHEN P. HEYMANN  
Assistant United States Attorney

Date: November 16, 2012

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 11-10260-NMG
	)	
AARON SWARTZ,	)	
	)	
Defendant	)	

MOTION FOR STATUS CONFERENCE

The United States moves this Court to hold a status conference to discuss:

- (1) Scheduling hearings for the Court to consider Defendant's motions to suppress and motion to dismiss;
- (2) Whether an evidentiary hearing is necessary to decide any of Defendant's motions and, if so, which ones;
- (3) If an evidentiary hearing is necessary, how to limit testimony so that the hearing is not a substantial pre-trial of the case and instead focuses on those facts which the Court has determined after reading the parties's briefs are material, in dispute and are necessary to resolve before ruling on the motions; and
- (4) Whether the timing of the hearing and probable timing of the resulting decisions counsels or necessitates briefly continuing the present trial date in this case.

The United States has conferred with counsel for the defendant and he does not oppose the scheduling of a status conference.

Respectfully submitted,

Carmen M. Ortiz  
United States Attorney

By: /s/ Stephen P. Heymann  
STEPHEN P. HEYMANN  
SCOTT L. GARLAND  
Assistant U.S. Attorneys

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/s/ Stephen P. Heymann  
STEPHEN P. HEYMANN  
Assistant United States Attorney

Date: November 30, 2012

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS**

UNITED STATES OF AMERICA,

v.

AARON SWARTZ,

Defendant.

No. 11-CR-10260-NMG

**DEFENDANT'S MOTION FOR LEAVE TO FILE REPLY BRIEFING AND EXHIBIT  
UNDER SEAL**

Pursuant to Local Rule 7.2, Defendant Aaron Swartz, through undersigned counsel, hereby moves for leave to file under seal: (1) Defendant's Reply in Support of Motions to Suppress and Motion to Dismiss Counts 1 and 2 of Superseding Indictment and (2) the accompanying exhibit to the Reply brief.

As grounds for this motion, Defendant states that the documents he seeks to file under seal include information concerning grand jury testimony and covered by the Protective Order in this case (the "confidential material"). Defendant simultaneously will file a redacted version of the Reply brief, omitting the confidential material, via the CM/ECF system.

Pursuant to Local Rule 7.2, Defendant requests that the confidential material be impounded until further order of the Court.

Dated: December 3, 2012

Respectfully submitted,

/s/ Elliot R. Peters

Elliot R. Peters (admitted *pro hac vice*)

Daniel Purcell (admitted *pro hac vice*)

Keker & Van Nest LLP

633 Battery Street

San Francisco, CA 94111

Tel.: (415) 391-5400

Fax: (415) 397-7188

Email: epeters@kvn.com

dpurcell@kvn.com

Michael J. Pineault

Clements & Pineault, LLP

24 Federal Street

Boston, MA 02110

Tel.: (857) 445-0135

Fax: (857) 366-5404

Email: mpineault@clementspineault.com

Attorneys for Defendant AARON SWARTZ

**CERTIFICATE OF SERVICE**

I hereby certify that this document filed through the CM/ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing and paper copies will be sent to those indicated as non-registered participants on December 3, 2012.

/s/ Elliot R. Peters

Elliot R. Peters



UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA,

v.

AARON SWARTZ,

Defendant.

No. 11-CR-10260-NMG

PUBLIC VERSION

**DEFENDANT'S REPLY IN SUPPORT OF MOTIONS TO SUPPRESS AND MOTION  
TO DISMISS COUNTS 1 AND 2 OF SUPERSEDING INDICTMENT**

**(Leave to File Granted by Electronic Order dated November 13, 2012)**

Aaron Swartz has moved to suppress five categories of evidence illegally obtained by the Government, including: (1) the "packet capture" of communications made by Swartz's ACER laptop while it was connected to the MIT network; (2) logs of network activity provided by MIT to law enforcement; (3) the fruits of the search of the exterior and interior of the ACER laptop while it was connected to the MIT network; and (4) the fruits of the search of the ACER laptop, Western Digital hard drive, and HP USB drive carried out pursuant to warrants first sought thirty-four days after the equipment was seized. Dkts. 59-63.<sup>1</sup> Also pending before the Court is Swartz's motion to dismiss Counts 1 and 2 of the Superseding Indictment. Dkt. 64. The Court should grant all these motions for the reasons laid out in the motions and this Reply.

Moreover, the Government's opposition briefs, Dkts. 81-82, make clear that many facts crucial to resolution of the pending motions remain in dispute. To resolve those disputes and decide the motions, the Court must hear testimony and receive evidence from witnesses with MIT, JSTOR, and the law enforcement agencies involved in the underlying investigation. Accordingly, Swartz respectfully asks the Court to hold an evidentiary hearing prior to deciding

---

<sup>1</sup> As to a fifth category of illegally obtained evidence, the Government has stated that it does not intend to offer either the network scan of the ACER laptop's ports or evidence derived from searches of Swartz's apartment and office during its case in chief. *See* Dkt. 81 at 34-35 n.23, 45. As a result, this Reply does not discuss the reasons why that evidence ought to be suppressed. Swartz maintains the objections to that evidence noted in his motion to suppress and reserves his right to challenge that evidence in the event the Government elects to offer it before or at trial.

the pending motions.

**I. THE EVIDENCE OBTAINED AS A RESULT OF THE WARRANTLESS SEARCHES MUST BE SUPPRESSED**

**A. Swartz had a reasonable expectation of privacy in his laptop computer and its electronic communications**

The Government contends Swartz had no reasonable expectation of privacy in his ACER laptop computer, its contents, and its electronic communications. But whether Swartz had a reasonable expectation of privacy can be evaluated only in the specific factual context of this case. It requires an analysis of MIT's specific policies and practices regarding computer use and privacy on the MIT campus, a community uniquely saturated with electronic devices. But as of now, there is nothing in the record before the Court describing this relevant context. The only reliable way to establish that context, and evaluate the reasonableness of Swartz's expectations, is for the Court to hear testimony from MIT officials and community members at an evidentiary hearing prior to the resolution of these motions.

Swartz believes such testimony will demonstrate he had both a subjective and objectively reasonable expectation of privacy in the ACER laptop and its contents when he placed the laptop in quiet and infrequently accessed locations—Room 16-004t in Building 16 (“Room 004”) and the locked office in the student center—where it was unlikely to be disturbed or stolen. Given MIT's open campus, virtually any room of which can be accessed by anyone walking off the street, Swartz specifically chose to place his computer somewhere where it would not be stolen, as it might be if he left it in a classroom or on a desk at the library. He sought and received permission from a student monitor to leave his computer in the locked office in the student center and, as further discussed in section I.B below, did not wrongfully enter Room 004. Swartz also returned to Room 004 twice over the course of three days to check on his property and password-protected his computer to provide an additional level of security. *See, e.g., United States v. Reeves*, 2012 WL 1806164, at \*8 (D.N.J. May 17, 2012) (password-protection was sufficient to show intent to maintain privacy in documents kept on computer).

It was also objectively reasonable for Swartz to expect that MIT would not violate (as it did) its obligations under the Stored Communications Act, the Wiretap Act, and the Massachusetts Wiretap Act by disclosing the electronic communications between his computer

and the MIT network at the direction of government agents. With respect to information in the MIT DHCP server logs, the objective reasonableness of Swartz's privacy expectation is further bolstered by MIT's own official policy, which specifies that DHCP logs will only be disclosed under the direction and approval of MIT's Office of the General Counsel—which presumably would ensure that MIT would not violate any electronic privacy laws. *See* IS&T Policies: DHCP Usage Logs Policy, <https://ist.mit.edu/about/policies/dhcp-usage-logs> (last visited Nov. 28, 2012). Even if Swartz's experience with software engineering made him aware that MIT might *monitor* his IP and MAC addresses during the time he was logged onto the network, there is no evidence that he knew or suspected that MIT would permanently record such information, much less share it with outsiders in violation of various applicable laws. *See* <http://ist.mit.edu/about/policies/dhcp-usage-logs> (last visited Nov. 30, 2012) (stating that MIT retains DHCP logs for only 30 days after creation); *see also United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007) (holding that the mere act of accessing a network does not extinguish privacy expectations). Consequently, Swartz had a reasonable expectation that MIT would not work hand-in-hand with law enforcement to illegally intercept, capture, and disclose his electronic communications while he was connected to MIT's open network as an authorized guest.

**B. The packet capture of the laptop computer cannot be justified under the trespasser exception to the warrant requirement**

The Government concedes that the January 4, 2011, packet capture of the ACER laptop's communications involved interception of the contents of those communications under color of law, and thus required a Title III order that the Secret Service failed to secure. Nonetheless, the Government attempts to salvage its warrantless seizure of the packet capture by arguing that Swartz "was a trespasser on MIT's system." Dkt. 81 at 23-25. The Government is wrong on the facts. All the purportedly undisputed "facts" asserted by the Government in support of its trespasser argument are either provably false or hotly disputed, which is yet another reason for the Court to hold an evidentiary hearing before deciding the pending motions.

The Government begins by erroneously claiming that Swartz physically trespassed onto MIT's campus, supporting this assertion by appending a single photograph of a single door somewhere on the MIT campus that happens to have a "no trespassing" sign. *See* Dkt. 81-8.

Apart from the fact that this image is undated and unauthenticated,<sup>2</sup> the Government neglects to mention that, in addition to this one door, there are myriad ways for anyone to gain access to Building 16's basement, including many that do not require entrance from the street. All of MIT's main buildings, including Building 16, are freely accessible through an extensive network of tunnels and hallways. More importantly, the Government does not dispute that MIT maintains an open campus. MIT affirmatively invites the public to visit its campus, tour its buildings, and attend lectures and events throughout the year, and so merely entering campus public spaces cannot be considered a trespass. *See* <http://mitadmissions.org/visit/visit> (last visited Nov. 26, 2012) ("The MIT campus is open to the public year-round."); <http://web.mit.edu/institute-events/visitor/> (last visited Nov. 26, 2012); [REDACTED] Neither Building 16 nor its basement was locked; both were readily accessible by any member of the public.<sup>3</sup>

Moreover, the Government's claim that Swartz accessed Room 004 by opening "locked steel doors" is fictional. Contemporaneous video surveillance taken from inside the room contradicts this characterization. That footage reveals that the doors to the room were often left ajar, and were accessed by numerous individuals at different times, none of whom needed or used a key to do so. [REDACTED]

[REDACTED] Room 004 itself was clearly accessible to the public, as evidenced by the large amount of graffiti on its walls, *see* Dkt. 81-10, and surveillance footage of unidentified individuals accessing the room or using it to store garbage bags.

Finally, the Government incorrectly asserts that Swartz "trespassed" on MIT's network. But MIT's network was open to anyone present on its campus, regardless of whether they had any affiliation with MIT or other formal reason to be there. *See* Dkt. 68, Ex. 3 (stating that visitor access is provided on-demand to anyone who walks onto campus) [REDACTED]

[REDACTED] Further, access to the network did not require any user identification,

<sup>2</sup> The Government has not authenticated any of the images and screen shots cited as exhibits in its opposition with an accompanying declaration. Many of the images and screen shots lack any information identifying the date they were taken. To the extent the Government wants to rely on these images to defeat suppression, it must lay some foundation permitting the Court to believe they are what the Government asserts they are.

<sup>3</sup> In addition, Swartz was not a mere visitor to MIT; he was an established member of the MIT community who had given a guest lecture, audited MIT classes, worked on projects with MIT professors, and attended events on campus on multiple occasions.

password, or other verification. While the Government points to Defendant's use of pseudonyms when registering for network access, that makes no difference for purposes of access. MIT never took any steps to actually verify the identity of network users prior to granting access or restrict use by people entering pseudonyms when they logged on. *See* Dkt. 68, Ex. 3. Swartz was not a trespasser at MIT and is entitled to the full protections of the Fourth Amendment.

**C. The Government has failed to excuse law enforcement's decision to conduct warrantless searches of the computer's interior**

The Government throws out a variety of explanations for the investigators' failure to seek a warrant to open up and search Defendant's computer in hopes that one will stick. But neither the plain view doctrine nor MIT's consent to search Room 004 justify law enforcement's decision to open and inspect the computer while it was in the room, rather than disconnecting it from the network and seizing it for a later search pursuant to a warrant. The Government's argument that the search was constitutionally valid because Swartz's computer was "wrongfully" present in Room 004 is unavailing, for the same reasons Swartz was not a trespasser.

The Government also argues that the investigators' decision to open the computer was justified by "exigent circumstances," because a computer's random access memory ("RAM") information is lost when the computer is turned off. *See* Dkt. 81 at 35-36. But there was no exigency here. Investigators could have seized the computer, disconnected it from the network, and obtained a warrant to search its RAM prior to powering the computer down. There was no imminent risk that the computer would spontaneously shut down during the time that it was within law enforcement's control. Instead, the Government created its own "exigent circumstances" by choosing to leave the computer connected to the network and inside Room 004 in an attempt to lure the computer's owner into revealing himself, seeking an investigatory benefit in exchange for the risk that the owner would turn the computer off. Accordingly, the Government cannot justify the search of the computer's interior without a warrant and the fruits of that search must be suppressed.

**II. THE DELAY IN OBTAINING WARRANTS TO SEARCH DEFENDANT'S COMPUTER EQUIPMENT VIOLATED THE FOURTH AMENDMENT**

The Secret Service's *34-day delay* in obtaining search warrants for (1) the ACER laptop; (2) the Western Digital hard drive; and (3) the HP USB drive rendered seizure of those items

unreasonable under the Fourth Amendment. Accordingly, the Court must suppress the fruits of the searches eventually conducted on those items.

The Government attempts to avoid the consequences of its unreasonable delay with four specious arguments. *First*, it argues the Cambridge Police were entitled to hold the laptop, hard drive, and USB drive for an unlimited period of time as physical evidence of computer crimes, larceny, and breaking and entering, analogizing the seized items to “a bag of burglar tools.” Dkt. 81 at 47. But this same argument was recently rejected, and rightly, in *United States v. Shaw*, 2012 WL 844075, at \*3 (N.D. Ga. Feb. 10, 2012), which held that cell phones seized during an arrest were not evidence of a crime in and of themselves, because phones are not contraband and do not have evidentiary value apart from their contents.

Just as was true for the phones in *Shaw*, Swartz’s computer hardware is not contraband in and of itself. Unlike a burglar’s bag of tools, computers have a multitude of legitimate uses and play a routine and increasingly essential role in everyone’s daily life. *See United States v. Mitchell*, 565 F.3d 1347, 1351 (11th Cir. 2009) (observing that there is a strong possessory interest in computer hard drives because they are heavily relied upon for personal and business use). Moreover, the Government has not explained with any level of specificity *how* the computer hardware, as distinguished from its contents, offers any physical evidence of the charged crimes. *See Shaw*, 2012 WL 844075 at \*3; *see also United States v. Wright*, 2010 WL 841307, at \*10 (E.D. Tenn. Mar. 3, 2010) (“Ordinarily, of course, a suspect’s possession of a computer will have no evidentiary value apart from its contents.”).<sup>4</sup>

*Second*, the Government claims that the Secret Service’s unexplained delay cannot have harmed Swartz’s possessory interests in the computer media because he never asked the investigators for his equipment back. This makes no difference. A defendant’s Fourth Amendment rights do not depend and never have depended on whether he expressly seeks the

<sup>4</sup> Even if the Government had offered a specific reason that the laptop and hard drive amounted to physical evidence of a crime, rather than being of evidentiary value for their contents alone, there is absolutely no connection between the alleged Massachusetts crimes and Swartz’s possession of the HP USB drive at the time of his arrest. Possession of a USB drive while riding a bike on a public street is an entirely innocent activity and the investigators had no evidence that the USB drive was ever even present in Room 004. Accordingly, the drive’s seizure cannot conceivably be justified based on an argument that it was physical evidence *in and of itself* of computer crimes, breaking and entering, or larceny.



return of wrongly seized property. Courts routinely suppress evidence seized after unreasonable delays in applying for search warrants, even where the defendant never demanded return of his belongings. *See Shaw*, 2012 WL 844075 at \*3 (defendant's failure to request return of cell phones was immaterial to result); *see also United States v. Mitchell*, 565 F.3d 1347, 1348-53 (11th Cir. 2009); *United States v. Riccio*, 2011 WL 4434855, at \*1-\*3 (S.D. Cal. Sept. 23, 2011); *United States v. Rubinstein*, 2010 WL 2723186, at \*12-\*14 (S.D. Fla. June 24, 2010).<sup>5</sup> As Swartz pointed out in his motion, *see* Dkt. 63 at 4-5, courts have found delays much shorter than 34 days to be unreasonable and to require suppression. *See Mitchell*, 565 F.3d at 1350 (21-day delay in seeking search warrant was unreasonable).

*Third*, the Government remarkably suggests the Secret Service cannot be held responsible for its lackadaisical attitude toward seeking a search warrant because the Cambridge Police Department, not the Secret Service, was in possession of the computer equipment during the thirty-four day delay. It is telling that the Government fails to cite a single case in support of this proposition. Accepting this argument would allow one government agency to end-run Fourth Amendment requirements in the easiest manner imaginable—by leaving wrongly seized evidence in the possession of some other, closely cooperating government agency. Here, the Secret Service was plainly in charge of the investigation at MIT. It is absurd to suggest that it had no control over the seized computer equipment when its investigation directly resulted in that equipment being kept in the possession of the Cambridge Police. *See* Dkt. 68, Ex. 31 (report states that Secret Service Agent Pickett apprehended and handcuffed Swartz); Dkt. 68, Ex. 15 (report states that Pickett examined ACER laptop before turning it over in evidence bag to MIT Police). [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

*Finally*, the Government asserts that the Secret Service's delay in seeking a warrant was

<sup>5</sup> In support of its contention that Swartz lacked a possessory interest in his computer equipment, the Government asserts that Swartz left his laptop unaccompanied for three months. This is speculation, as the Government has never pleaded any facts, as opposed to stating conclusions, indicating that Swartz's laptop was left unattended at any time prior to January 4, 2011.



justified because the computer crime at issue was “complex” and involved gathering “technical and specialized information.” Dkt. 18 at 53-54. But the Government cannot simply assert this conclusion without proving it with evidence. In order to outweigh Swartz’s strong possessory interest in his equipment, the Government must present a “compelling justification” for the delay in applying for a warrant. *Mitchell*, 565 F.3d at 1351; *see also Riccio*, 2011 WL 4434855 at \*1 (faulting the government for not presenting any specific facts to explain need for delay). The Government offered no declaration from any of the officers involved in the pre-warrant investigation regarding technical complexity, nor pointed to even one piece of technical information presented in the warrants that necessitated over a month of delay between the seizure of the items and the application for a search warrant.

Moreover, the warrant applications specifically averred that Secret Service Agent Pickett was specially trained in the investigation of crimes involving unauthorized intrusions into computer networks. *See, e.g.*, Dkt. 68, Ex. 30. The Government has not indicated any unique circumstances that made this investigation particularly difficult for an agent with such extensive experience in the field of computer crimes. As it stands, the Government’s response is simply a bare-bones conclusion that does not establish a “compelling justification” for the delay. At the very least, the Court should hear testimony from Agent Pickett regarding why the Secret Service delayed at such length before applying for a warrant.

### **III. THE WIRE FRAUD COUNTS MUST BE DISMISSED BECAUSE THE GOVERNMENT HAS FAILED TO ALLEGE A MISREPRESENTATION**

The Court should also dismiss Counts 1 and 2 of the Superseding Indictment, because—as the Government’s opposition makes clear—those wire-fraud counts are an improper attempt to apply an amorphous, overly broad federal statute that simply does not fit the charged conduct. The wire fraud charges cannot survive Defendant’s motion to dismiss because, as the Government concedes, wire fraud requires a material misrepresentation. *See* Dkt. 82 at 2-3 (list of alleged misrepresentations); *see also Neder v. United States*, 527 U.S. 1, 16 (1999) (to be material, false statement must have natural tendency to influence, or be capable of influencing, decision of body to which it was addressed). The indictment does not sufficiently allege any such misrepresentation.

Nothing about Swartz's access to MIT's network, or to JSTOR through MIT's network, depended on or was influenced by any alleged misrepresentation. MIT's open network permits any person on MIT's premises free and full access, without requiring any user identification or password. At the time of the alleged offenses, MIT's network asked a user to enter a name and email address, but took no steps to verify that name or address, or to grant or deny access depending on the name or address entered. Dkt. 68, Ex. 3. An MIT guest would obtain the same full access to the MIT network whether she entered her real name or "Donald Duck" in the name field. Accordingly, Swartz's alleged use of pseudonyms cannot possibly have materially influenced MIT's decision to grant him access to the network. And, once Swartz was on the MIT network as an authorized guest user, he similarly gained full access to the JSTOR database under the terms of JSTOR's agreement with MIT. In fact, JSTOR's Terms and Conditions of Use specifically define "authorized users" under university contracts as including "on-site users physically present on the Institutional Licensee's premises." Dkt. 81-3. Consequently, Swartz was an authorized JSTOR user merely by virtue of his presence on MIT's campus.

Likewise, a computer's IP is not a constant, unalterable feature, like an automobile's VIN number. A computer is assigned an IP address each time that computer accesses a network, and this results in the same computer using a different IP address from day to day. Moreover, all major computer operating systems makes it trivially simple for any user to change the computer's IP address, which ability is useful for troubleshooting purposes when the computer is having difficulty communicating with a network. Until recently, computer users were frequently required to manually enter an IP address in order to connect the machine to the Internet. Neither is a MAC address a static feature of a device. Not only can a MAC address be changed with a few clicks of a mouse in every major operating system, the ability to change a MAC address is a required feature of personal computer hardware. Accordingly, neither an IP addresses nor a MAC address is necessarily associated with, or can be used as a reliable identifier for, any given user. A change to either does not represent any misrepresentation about a user's identity.

The Government also contends that Swartz violated JSTOR's terms of service by using a software program to create multiple JSTOR sessions and download a large volume of articles. In the first place, the Government offers no evidence that Swartz was ever presented with, much

less accepted, JSTOR's terms of service. [REDACTED]

[REDACTED] Finally, the Government has merely alleged that Swartz hid his computer in a basement room, not that he misrepresented its location to anyone. Because the Government has not alleged any affirmative misrepresentation by Swartz, it has not pleaded a wire fraud claim, and the Court should dismiss Counts 1 and 2.<sup>6</sup>

#### IV. CONCLUSION

For all the above reasons, the Court should either grant Swartz's motions to suppress and motion to dismiss or conduct an evidentiary hearing regarding those motions to resolve any factual disputes necessary to resolve those motions.

Respectfully submitted,

Dated: December 3, 2012

By: /s/ Elliot R. Peters

Elliot R. Peters (*pro hac vice*)  
Daniel Purcell (*pro hac vice*)  
KEKER & VAN NEST LLP  
633 Battery Street  
San Francisco, CA 94111-1809  
Telephone: 415 391 5400  
Facsimile: 415 397 7188  
[epeters@kvn.com](mailto:epeters@kvn.com)  
[dpurcell@kvn.com](mailto:dpurcell@kvn.com)

Michael J. Pineault  
Clements & Pineault, LLP  
24 Federal Street  
Boston, MA 02110  
Telephone: 857 445 0135  
Facsimile: 857 366 5404  
[mpineault@clementspineault.com](mailto:mpineault@clementspineault.com)

*Attorneys for Defendant AARON SWARTZ*

<sup>6</sup> If the Court grants Swartz's motion to dismiss, the Government will remain free to pursue the ten separate counts in the Superseding Indictment alleging violations of 18 U.S.C. § 1030.

**CERTIFICATE OF SERVICE**

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing, and paper copies will be sent on December 3, 2012 to those indicated as non-registered participants.

Dated: December 3, 2012

/s/ Elliot R. Peters  
Elliot R. Peters

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS**

UNITED STATES OF AMERICA,

Plaintiff,

v.

AARON SWARTZ,

Defendant.

Crim. No. 11-CR-10260-NMG

**DEFENDANT'S MOTION FOR CONTINUANCE OF TRIAL DATE  
AND EXPERT DISCLOSURE DEADLINE**

Defendant Aaron Swartz hereby respectfully moves for a 120 day continuance of the trial date of this matter from February 4, 2013 to June 10, 2013, or the next available date on the Court's calendar after that date and for a continuance of his deadline for expert disclosure from December 11, 2012 to February 25, 2013. In support of this motion, Swartz submits the accompanying memorandum of law.

Dated: December 3, 2012

Respectfully submitted,

/s/ Elliot R. Peters

Elliot R. Peters (admitted *pro hac vice*)

Daniel Purcell (admitted *pro hac vice*)

Keker & Van Nest LLP

633 Battery Street

San Francisco, CA 94111

Tel.: (415) 391-5400

Fax: (415) 397-7188

Email: epeters@kvn.com

dpurcell@kvn.com

Michael J. Pineault  
Clements & Pineault, LLP  
24 Federal Street  
Boston, MA 02110  
Tel.: (857) 445-0135  
Fax: (857) 366-5404  
Email: mpineault@clementspineault.com

Attorneys for Defendant AARON SWARTZ

**CERTIFICATION PURSUANT TO LOCAL RULE 7.1(A)(2)**

I hereby certify that counsel for Swartz has conferred with counsel for the Government in an attempt to resolve or narrow the issues presented by this motion, but were unable to reach agreement.

/s/ Elliot R. Peters

Elliot R. Peters

**CERTIFICATE OF SERVICE**

I hereby certify that this document filed through the CM/ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing and paper copies will be sent to those indicated as non-registered participants on December 3, 2012.

/s/ Elliot R. Peters  
ELLIOT R. PETERS



**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS**

UNITED STATES OF AMERICA,

Plaintiff,

v.

AARON SWARTZ,

Defendant.

Crim. No. 11-CR-10260-NMG

**MEMORANDUM IN SUPPORT OF DEFENDANT'S MOTION FOR CONTINUANCE  
OF TRIAL DATE AND EXPERT DISCLOSURE DEADLINE**

Defendant Aaron Swartz hereby respectfully moves for a 120 day continuance of the trial date of this matter from February 4, 2013 to June 10, 2013, or the next available date on the Court's calendar after that date and for a continuance of his deadline for expert disclosure from December 11, 2012 to February 25, 2013.

Trial of this matter is presently set for February 4, 2013. Substantial work still needs to be done, both by the parties and by the Court, before the case can be tried. The requested continuance, the first such request by Swartz, would facilitate the orderly administration of justice and permit counsel for Swartz to complete the work necessary to prepare efficiently to present this case to the jury during trial. There are several separate reasons why this request is meritorious and in the interests of justice.

*First*, Swartz has filed motions to suppress, with his Reply filed on the same date as this motion. These motions require a hearing to evaluate the evidence presented by the government. As set forth in the Reply, the issues raised by the Government in opposition to the motions require the testimony of witnesses from MIT, JSTOR and likely several law enforcement agencies. Both sides in this case, and the Court, need to know the outcomes of those motions in order sensibly to prepare for trial. Counsel for Swartz has several hearings set, and a weeklong arbitration in another matter, during December 2012, so it is unlikely—even without considering

this Court's extremely busy schedule—that a hearing could be calendared before January 2013, at the earliest. Instead, Swartz respectfully suggests that the current February 4, 2013 trial date, on which all parties are obviously available, be used to conduct the suppression hearing, followed by a June trial.

*Second*, this is not a garden-variety criminal case involving factual issues that are readily intelligible to any layperson. Instead, this is a highly technical computer-fraud case that will require the parties to present, and the Court and the jury to understand and evaluate, complex issues regarding the operation of computer networks, how those networks are accessed, the operation and identification of individual computers (including their MAC addresses, IP addresses, and “BASH” histories), and the operation of computer programs which cause the downloading of content from network servers. On November 18, 2012 the government disclosed a 44-page report summarizing the expected testimony of its expert witness on some of these topics. Swartz's expert disclosure is presently due December 11, 2012. Due to the complexity of the issues, not to mention the due diligence and expense associated with hiring an expert competent to opine on the issues addressed by the government's expert, Swartz has concerns about his ability to meet the December 11, 2012 deadline, and would be severely prejudiced if he were unable to do so. It is apparent that the government has been working extensively with its expert for many months in the preparation of his report. Swartz does not desire to produce an incomplete expert disclosure on December 11, then seek to amend it. He would rather have adequate time before trial to fully vet the technical issues with a qualified expert and then move forward. Swartz's ability to prepare an expert is further complicated by the issues identified in the following paragraph.

*Third*, the material necessary for the preparation of a complete expert disclosure and to adequately prepare for trial is not presently in the hands of the defense. While Swartz does not know what evidence the grand jury subpoenaed or what evidence the investigators obtained voluntarily from MIT and JSTOR, it is apparent that the materials the government obtained and produced in discovery are not nearly adequate to rebut the factual claims presented in the

government's oppositions to Swartz's suppression motions and to defend the case at trial. While the government has sought and obtained evidence from third parties to assist it in presenting its version of the truth, substantial additional relevant and evidentiary materials remain to be obtained by Swartz. Swartz is and has acted diligently in this regard, and the Court is aware of his efforts. But it is by no means certain that all the additional materials Swartz needs and is seeking to obtain will be in his hands within thirty days, much less by the expert disclosure deadline of December 11, 2012. Further, once any materials are received, Swartz needs to review them, produce those which are properly discoverable under Fed. R. Crim. P. 16, and then incorporate those documents into his expert's analysis and opinions. It is certain that this task cannot be completed by December 11, 2012, and Swartz has considerable doubts that it could be completed before the existing February 4, 2012 trial date.

For the foregoing reasons, and to assist the Court and the jury of making a fully informed and fair resolution of all issues in dispute, Swartz respectfully requests that trial of this case be continued from February 4, 2013 to June 10, 2013, that the date for Swartz's expert disclosure be continued from December 11, 2012 to February 25, 2013, and that the Court consider utilizing the current February 4, 2013 trial date for an evidentiary hearing on the Motions to Suppress.

Dated: December 3, 2012

Respectfully submitted,

/s/ Elliot R. Peters

Elliot R. Peters (admitted *pro hac vice*)

Daniel Purcell (admitted *pro hac vice*)

Keker & Van Nest LLP

633 Battery Street

San Francisco, CA 94111

Tel.: (415) 391-5400

Fax: (415) 397-7188

Email: epeters@kvn.com

dpurcell@kvn.com

Michael J. Pineault  
Clements & Pineault, LLP  
24 Federal Street  
Boston, MA 02110  
Tel.: (857) 445-0135  
Fax: (857) 366-5404  
Email: mpineault@clementspineault.com

Attorneys for Defendant AARON SWARTZ

**CERTIFICATE OF SERVICE**

I hereby certify that this document filed through the CM/ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing and paper copies will be sent to those indicated as non-registered participants on December 3, 2012.

/s/ Elliot R. Peters  
ELLIOT R. PETERS

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS**

UNITED STATES OF AMERICA,

Plaintiff,

v.

AARON SWARTZ,

Defendant.

Crim. No. 11-CR-10260-NMG

**DEFENDANT'S RESPONSE TO GOVERNMENT'S  
MOTION FOR A STATUS CONFERENCE**

As the Government accurately noted in its Motion for Status Conference in this case, Dkt. 85, Defendant Aaron Swartz agrees that it would be beneficial for the Court to hold a status conference. In particular, a status conference is likely to assist the Court in addressing scheduling issues relating to a hearing on Swartz's pending motions.

Swartz files this Response in order to inform the Court about certain conflicts in his lead counsel's schedule for the following month. Swartz has previously provided this information to the AUSAs handling the matter. It would be Swartz's strong preference for his lead trial counsel, Elliot Peters, to be able to attend any such status conference in person, and counsel will make all efforts to do so. Swartz therefore respectfully requests that the Court take these scheduling conflicts into account in scheduling a status conference, if the Court elects to hold one. Specifically, the undersigned counsel is unavailable during the week of December 3, 2012; has a full-day mediation on December 11, 2012; has hearings in California on both December 12 and 13, 2012; has an arbitration scheduled for the entire week of December 17, 2012; has a hearing in San Francisco on January 3, 2012; and has a sentencing in Sacramento, California on January 8, 2012. Swartz respectfully suggests that the Court hold a status conference on either January 10 or 11, 2012. AUSA Heymann has informed me that he considers this request "unreasonable" and that he would prefer an earlier status conference.

Dated: December 3, 2012

Respectfully submitted,

/s/ Elliot R. Peters

Elliot R. Peters (admitted *pro hac vice*)

Daniel Purcell (admitted *pro hac vice*)

Keker & Van Nest LLP

633 Battery Street

San Francisco, CA 94111

Tel.: (415) 391-5400

Fax: (415) 397-7188

Email: epeters@kvn.com

dpurcell@kvn.com

Michael J. Pineault

Clements & Pineault, LLP

24 Federal Street

Boston, MA 02110

Tel.: (857) 445-0135

Fax: (857) 366-5404

Email: mpineault@clementspineault.com

Attorneys for Defendant AARON SWARTZ



**CERTIFICATE OF SERVICE**

I hereby certify that this document filed through the CM/ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing and paper copies will be sent to those indicated as non-registered participants on December 3, 2012.

/s/ Elliot R. Peters  
ELLIOT R. PETERS

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4670424@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Order on Motion for Hearing  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 12/3/2012 at 4:54 PM EST and filed on 12/3/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** 91(No document attached)

**Docket Text:**

**Judge Nathaniel M. Gorton: ELECTRONIC ORDER entered granting [85] Motion for Hearing as to Aaron Swartz (1) (Patch, Christine)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Michael J. Pineault mpineault@clementspineault.com

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Matthias A. Kamber mkamber@kvn.com, ashen@kvn.com, plemos@kvn.com

Elliot R. Peters epeters@kvn.com, apicar@kvn.com, efiling@kvn.com, kbringola@kvn.com, klovet@kvn.com

Daniel E. Purcell dpurcell@kvn.com

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4670426@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Notice of Hearing  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 12/3/2012 at 4:55 PM EST and filed on 12/3/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** 92(No document attached)

**Docket Text:**

**ELECTRONIC NOTICE OF HEARING as to Aaron Swartz Status Conference set for 12/14/2012 02:00 PM in Courtroom 4 before Judge Nathaniel M. Gorton. (Patch, Christine)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Michael J. Pineault mpineault@clementspineault.com

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Matthias A. Kamber mkamber@kvn.com, ashen@kvn.com, plemos@kvn.com

Elliot R. Peters epeters@kvn.com, apicar@kvn.com, efiling@kvn.com, kbringola@kvn.com, klovett@kvn.com

Daniel E. Purcell dpurcell@kvn.com

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4670936@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Order on Motion for Leave to File  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 12/4/2012 at 9:38 AM EST and filed on 12/4/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** 93(No document attached)

**Docket Text:**

**Judge Nathaniel M. Gorton: ELECTRONIC ORDER entered granting [86] Motion for Leave to File Reply Briefing and Exhibit Under Seal. (Patch, Christine)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Michael J. Pineault mpineault@clementspineault.com

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Matthias A. Kamber mkamber@kvn.com, ashen@kvn.com, plemos@kvn.com

Elliot R. Peters epeters@kvn.com, apicar@kvn.com, efiling@kvn.com, kbringola@kvn.com, klovett@kvn.com

Daniel E. Purcell dpurcell@kvn.com

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4671309@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Reply to Response  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 12/4/2012 at 11:01 AM EST and filed on 12/4/2012

**Case Name:** USA v. Swartz  
**Case Number:** 1:11-cr-10260-NMG  
**Filer:** Dft No. 1 – Aaron Swartz  
**Document Number:** 94

**Docket Text:**

**SEALED REPLY in Support of [63] MOTION to Suppress , [61] MOTION to Suppress , [62] MOTION to Suppress , [64] MOTION to Dismiss , [59] MOTION to Suppress , [60] MOTION to Suppress by Aaron Swartz. (Attachments: # (1) Exhibit 1, # (2) Cover Letter)(Moore, Kellyann)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Michael J. Pineault mpineault@clementspineault.com

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Matthias A. Kamber mkamber@kvn.com, ashen@kvn.com, plemos@kvn.com

Elliot R. Peters epeters@kvn.com, apicar@kvn.com, efiling@kvn.com, kbringola@kvn.com, klovet@kvn.com

Daniel E. Purcell dpurcell@kvn.com

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

The following document(s) are associated with this transaction:

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 11-10260-NMG
	)	
AARON SWARTZ,	)	
	)	
Defendant	)	

GOVERNMENT’S OPPOSITION TO DEFENDANT’S MOTION FOR  
A CONTINUANCE OF TRIAL DATE AND EXPERT DISCLOSURE DEADLINE

The Court should deny Swartz’s request to put off his trial for another three months to the extent it is based on the amount of trial preparation he still has left to do or on his defense counsels’ schedules. The United States understands that Swartz retained his third set of trial counsel three months before trial, but these deadlines were present when they joined the case and informed the Court on November 8<sup>th</sup> that they sought no alteration of the present schedule due to their substitution as counsel. (Dkt. No. 73, p. 2).

The Court should deny Swartz’s request for an additional two and a half months to comply with expert disclosure. Swartz agreed to the present schedule for expert disclosure on March 8<sup>th</sup> (Dkt. No. 34, ¶ 6) and it has been incorporated in every interim status report by the Court since. He was provided forensic reports attaching material files recovered from his laptop computer and USB thumb drive as part of automatic discovery, over a year ago.

The Court should continue the trial date only for so long as will allow the Court to hear and decide Swartz's motions to suppress and dismiss, and the parties thereafter to craft their cases in light of the Court's rulings.

Respectfully submitted,

CARMEN M. ORTIZ  
United States Attorney

By: /s/ Stephen P. Heymann  
STEPHEN P. HEYMANN  
SCOTT L. GARLAND  
Assistant U.S. Attorney

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/s/ Stephen P. Heymann  
STEPHEN P. HEYMANN  
Assistant U.S. Attorney

Date: December 5, 2012



MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4688584@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Status Conference  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 12/14/2012 at 2:38 PM EST and filed on 12/14/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** 96(No document attached)

**Docket Text:**

**ELECTRONIC Clerk's Notes for proceedings held before Judge Nathaniel M. Gorton: Interim Status Conference as to Aaron Swartz held on 12/14/2012 (Attorneys present: Hayman, Peters, Pineault, Purcell (by phone). )Court Reporter Name and Contact or digital recording information: Cheryl Dahlstrom (617-951-4555). Court is in session. Court hears from the parties as to the necessity of an evidentiary hearing. Court orders hearing on 1/25/2013 at 1:00 p.m. Experts designated by 1/25/2013. Trial to begin on 4/1/2013. (Hohler, Daniel)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Michael J. Pineault mpineault@clementspineault.com

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Matthias A. Kamber mkamber@kvn.com, ashen@kvn.com, plemos@kvn.com

Elliot R. Peters epeters@kvn.com, apicar@kvn.com, efiling@kvn.com, kbringola@kvn.com, klovett@kvn.com

Daniel E. Purcell dpurcell@kvn.com, jwinars@kvn.com

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4688594@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Notice of Hearing  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 12/14/2012 at 2:40 PM EST and filed on 12/14/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** 97(No document attached)

**Docket Text:**

**ELECTRONIC NOTICE OF HEARING as to Aaron Swartz Evidentiary Hearing set for 1/25/2013 01:00 PM in Courtroom 4 before Judge Nathaniel M. Gorton. Jury Trial set for 4/1/2013 09:00 AM in Courtroom 4 before Judge Nathaniel M. Gorton. (Hohler, Daniel)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Michael J. Pineault mpineault@clementspineault.com

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Matthias A. Kamber mkamber@kvn.com, ashen@kvn.com, plemos@kvn.com

Elliot R. Peters epeters@kvn.com, apicar@kvn.com, efiling@kvn.com, kbringola@kvn.com, klovet@kvn.com

Daniel E. Purcell dpurcell@kvn.com, jwinars@kvn.com

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

United States District Court  
District of Massachusetts

_____	)	
UNITED STATES,	)	
	)	
v.	)	
	)	Criminal Case No.
AARON SWARTZ,	)	11-10260-NMG
Defendant.	)	
_____	)	

NOTICE

GORTON, J.

This is to memorialize the Court's rulings during a status conference held December 14, 2012.

The Court will hold an evidentiary hearing with respect to defendant's motions to suppress (Docket Nos. 59 - 63) on Friday, January 25, 2013 at 1:30 P.M. The hearing will be completed before the close of business that day with time allotted equally to each party.

The subject matter of the evidentiary hearing will be limited to the following subjects:

- (1) the basis for the government's 34-day delay in obtaining a warrant to search the contents of defendant's seized computer equipment;
- (2) whether defendant physically trespassed on MIT's property, with particular regard to the placement of defendant's laptop inside a wiring closet in Building 16; and
- (3) whether defendant abandoned the laptop he left at MIT.

Defendant's motion to continue the trial and the deadline to

disclose experts (Docket No. 88) is **ALLOWED, in part, and DENIED, in part.** The deadline for defendant's disclosure of expert witnesses is extended from December 11, 2012 until January 25, 2013. The trial will commence on Monday, April 1, 2013 at 9:00 A.M.

**So ordered.**

  
\_\_\_\_\_  
Nathaniel M. Gorton  
United States District Judge

Dated December 17, 2012

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4691957@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Set/Reset Deadlines/Hearings  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 12/18/2012 at 9:41 AM EST and filed on 12/18/2012

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** 99(No document attached)

**Docket Text:**

**Set/Reset Deadlines/Hearings as to Aaron Swartz: Expert Witness List due by 1/25/2013. Evidentiary Hearing set for 1/25/2013 01:30 PM in Courtroom 4 before Judge Nathaniel M. Gorton. (Moore, Kellyann)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Michael J. Pineault mpineault@clementspineault.com

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Matthias A. Kamber mkamber@kvn.com, ashen@kvn.com, plemos@kvn.com

Elliot R. Peters epeters@kvn.com, apicar@kvn.com, efiling@kvn.com, kbringola@kvn.com, klovett@kvn.com

Daniel E. Purcell dpurcell@kvn.com, jwinars@kvn.com

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS**

UNITED STATES OF AMERICA,

v.

AARON SWARTZ,

Defendant.

No. 11-CR-10260-NMG

**DEFENDANT AARON SWARTZ'S MOTION FOR LEAVE TO FILE SUPPLEMENTAL  
MEMORANDUM IN SUPPORT OF MOTIONS TO SUPPRESS**

Aaron Swartz requests permission to supplement the record related to his pending Motion to Suppress evidence obtained from the ACER laptop, Western Digital hard drive, and HP USB drive (Dkt. 63) with the accompanying Supplemental Memorandum (Ex. 1). The Supplemental Memorandum addresses a document recently produced to undersigned counsel by the Government, which document directly refutes arguments made by the Government in opposing suppression of the laptop, hard drive, and USB drive. The document was produced by the government on December 14, 2012, eleven days after Swartz filed his reply brief on December 3, 2012. Prior to December 14, Swartz was unaware of the document's existence and therefore did not have the opportunity to present the document to the Court in his motion papers.

Accordingly, and as more fully explained in the attached Supplemental Memorandum, Swartz believes that the recently-disclosed document is necessary for full consideration of his motion, and respectfully requests that the Court permit the filing of the Supplemental Memorandum.

**CERTIFICATION PURSUANT TO LOCAL RULE 7.1**

The undersigned counsel certifies that he has conferred with Government counsel concerning this motion, and that Government counsel has assented to defendant's request for

leave to file a supplemental brief. More specifically, Government counsel has asked that the following language be included in this certification: “The United States does not object to the Defendant’s request to supplement his pleadings and will respond to the factual assertions and arguments they contain within 14 days, as contemplated by the Local Rules.”

Dated: January 7, 2013

Respectfully submitted,

/s/ Elliot R. Peters

Elliot R. Peters (admitted *pro hac vice*)

Daniel Purcell (admitted *pro hac vice*)

Keker & Van Nest LLP

633 Battery Street

San Francisco, CA 94111

Tel.: (415) 391-5400

Fax: (415) 397-7188

Email: epeters@kvn.com

dpurcell@kvn.com

Michael J. Pineault

Clements & Pineault, LLP

24 Federal Street

Boston, MA 02110

Tel.: (857) 445-0135

Fax: (857) 366-5404

Email: mpineault@clementspineault.com

Attorneys for Defendant AARON SWARTZ



**CERTIFICATE OF SERVICE**

I hereby certify that this document filed through the CM/ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing and paper copies will be sent on January 7, 2013 to those indicated as non-registered participants.

/s/ Elliot R. Peters

Elliot R. Peters

# EXHIBIT 1

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS**

UNITED STATES OF AMERICA,

v.

AARON SWARTZ,

Defendant.

No. 11-CR-10260-NMG

**DEFENDANT AARON SWARTZ'S SUPPLEMENTAL MEMORANDUM IN SUPPORT  
OF MOTIONS TO SUPPRESS**

Aaron Swartz requests the Court's permission to supplement his Motions to Suppress and Dismiss (Dkts. 59-63) with a critical document only recently produced to Swartz by the Government. *See* Ex. A. The Government produced this document to Swartz for the first time in a letter dated December 14, 2012—after both the December 3, 2012, filing deadline for Swartz's reply brief and the December 14, 2012 hearing where this Court considered whether to hold, and ordered, an evidentiary hearing on Swartz's motions to suppress evidence.

The document at issue is an email from Secret Service Agent Michael Pickett to AUSA Stephen Heymann on January 7, 2011, *one day* after the Cambridge Police's January 6, 2011 seizure of an ACER laptop, Western Digital hard drive, and HP USB drive from the MIT campus. Ex. A. In the email, Agent Pickett reports to AUSA Heymann that no one had yet sought a warrant to search the computer or flash drive, but that he was "prepared to take custody of the laptop anytime" after it was processed for prints by the Cambridge Police on the morning of January 7, "or whenever you [Heymann] feel is appropriate." *Id.*

This email directly refutes the Government's Opposition to Swartz's pending motion to suppress evidence obtained from the laptop, hard drive, and USB drive. Dkt. 63. Swartz's motion is based on the Government's failure to obtain a search warrant for those items until February 9, 2011—*34 days* after the seizure and 33 days after the email exchange between Agent

Pickett and AUSA Heymann. In its Opposition, the Government argued that the 34-day delay was the fault of the Cambridge Police, not the Secret Service, and cannot be imputed to the federal Government. Specifically, the Government wrote:

The Secret Service did not seize [Swartz's] laptop, hard drive, or USB drive on January 6, 2011; the Cambridge Police Department did. ***Nor did the Secret Service possess this equipment before obtaining the warrants; the Cambridge Police Department did.*** Thus, the United States did not affect Swartz's possessory interest in his equipment until it executed warrants. ... Swartz cannot simply morph allegations that local police held evidence too long in a local prosecution into a claim that federal law enforcement officers did so in a subsequent federal case.

Dkt. 81 at 52-53 (emphasis added).

The newly-disclosed email shows that the Government's claim that it had no control over the seized equipment until on or shortly before February 9, 2011 is factually inaccurate. Agent Pickett's email makes clear that the Government had actual control over all the computer hardware at issue as of January 7, 2011—the day after the seizure—and could have taken physical custody of that hardware at any time. Moreover, the email shows that the lead prosecutor in this case not only was aware of this, but was personally directing the Secret Service regarding whether and when to take physical custody of the hardware.

Accordingly, this recently-produced email is not merely relevant to the pending motions to suppress, it directly refutes the Government's excuse for the 34-day delay. It shows that the Government not only had control over the hardware as of January 7, 2011, but was fully aware at that point of the hardware's evidentiary significance to this prosecution and its need to seek a search warrant. The Government could and should have sought and obtained a warrant promptly at that point. It certainly has no excuse for waiting over a full month to do so.

Finally, Swartz could not have submitted the email along with the pending motions or his reply papers, because—despite the email's relevance to the issues before the Court—the Government did not produce the email until December 14, 2012. Swartz has always diligently sought all available discovery in this case. Had the Government timely produced this email, Swartz would have submitted it to the Court at his earliest opportunity and also would have used

the email at the December 14, 2012 hearing. For all these reasons, Swartz requests that the Court consider the email in deciding Swartz's pending motions to suppress, so the Court may resolve the issues presented on a full factual record.

Dated: January 4, 2013

Respectfully submitted,

/s/ Elliot R. Peters

Elliot R. Peters (admitted *pro hac vice*)

Daniel Purcell (admitted *pro hac vice*)

Keker & Van Nest LLP

633 Battery Street

San Francisco, CA 94111

Tel.: (415) 391-5400

Fax: (415) 397-7188

Email: epeters@kvn.com

dpurcell@kvn.com

Michael J. Pineault

Clements & Pineault, LLP

24 Federal Street

Boston, MA 02110

Tel.: (857) 445-0135

Fax: (857) 366-5404

Email: mpineault@clementspineault.com

Attorneys for Defendant AARON SWARTZ

**CERTIFICATE OF SERVICE**

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing, and paper copies will be sent on January 7, 2013 to those indicated as non-registered participants.

Dated: January 7, 2013

/s/ Elliot R. Peters

Elliot R. Peters

# **EXHIBIT A**





**U.S. Department of Justice**

***Carmen M. Ortiz***  
*United States Attorney*  
*District of Massachusetts*

*Main Reception: (617) 748-3100*

*John Joseph Moakley United States Courthouse*  
*1 Courthouse Way*  
*Suite 9200*  
*Boston, Massachusetts 02210*

December 14, 2012

Elliot R. Peters  
Keker & Van Nest LLP  
633 Battery Street  
San Francisco, CA 94111-1809  
Via hand delivery

Re: U.S. v. Aaron Swartz

Dear Mr. Peters:

Enclosed you will find an e-mail which I came across while collecting supplemental discovery materials for you in the Swartz case. (The e-mail has been redacted, eliminating my communication to the agent and contact information. Mike Halsall, David Newman and Jay Perault, as with other MIT employees in this case, may be contacted through their counsel, Robert Ullman.) Because I thought you might find it useful in light of arguments in your recently filed reply brief, I am providing it to you early while I continue to go through the remainder of the materials.

Very truly yours,

CARMEN M. ORTIZ  
United States Attorney

By:

  
STEPHEN P. HEYMANN  
Assistant U.S. Attorney

**From:** MICHAEL PICKETT (BOS) <Michael.Pickett@usss.dhs.gov>  
**Sent:** Friday, January 7, 2011 3:25 PM (GMT)  
**To:** Heymann, Stephen (USAMA) <Stephen.Heymann@usdoj.gov>  
**Subject:** RE: Swartz Case

---

The laptop and external hard drive have been logged into evidence with MIT police. Cambridge Police will take the laptop and hard drive to process them for prints this morning. I am prepared to take custody of the laptop anytime after it has been processed for prints or whenever you feel is appropriate. As far as I know no one has sought a warrant for the examination of the computer, the cell phone that was on his person or the 8gb flash drive that was in his backpack. FYI the laptop and external hard drive were not on his person when he was arrested. They were traced by the laptop MAC address on the network, in a computer room in the MIT student center.

Mike Halsall has already provided me with a copy of the flow traffic. David Newman has made the packet capture available for download. I will download it today.

I will ask Mike Halsall for a copy of the surveillance.

Jay A Perault is the Captain from MIT Police that has been working with me during this investigation and was present during the arrest of Aaron Swartz.

Michael S. Pickett  
U.S. Secret Service  
Boston Field Office

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 11-10260-NMG
	)	
AARON SWARTZ,	)	
	)	
Defendant	)	

MOTION FOR LEAVE TO FILE A RESPONSE TO NEW CONTENTIONS IN  
DEFENDANT'S SUPPLEMENTAL MEMORANDUM

The government requests permission to file the attached brief response to new contentions made by the Defendant in his Supplemental Memorandum in Support of his Motion to Suppress. The defendant does not object to the filing of a pleading similar in length to his own and directed solely to the matters he addresses in his Supplemental Memorandum.

Respectfully submitted,

Carmen M. Ortiz  
United States Attorney

By: /s/ Stephen P. Heymann  
STEPHEN P. HEYMANN  
SCOTT L. GARLAND  
Assistant U.S. Attorneys

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/s/ Stephen P. Heymann  
STEPHEN P. HEYMANN  
Assistant United States Attorney

Date: January 9, 2013

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 11-10260-NMG
	)	
AARON SWARTZ,	)	
	)	
Defendant	)	

GOVERNMENT’S RESPONSE TO DEFENDANT’S SUPPLEMENTAL MEMORANDUM  
IN SUPPORT OF HIS MOTION TO SUPPRESS No. 5

The e-mail that Defendant Swartz’s supplemental memorandum cites as paramount to his fifth motion to suppress is relevant, but not nearly as important as he tries to make it out to be. In that January 7, 2011 e-mail, Secret Service Special Agent Pickett said that he was prepared to take custody of the equipment at issue — a laptop, an attached hard drive and a USB storage device — after it was processed for fingerprints or anytime thereafter.

First, Swartz claims that this contradicts the Government’s representation that “Nor did the Secret Service possess this equipment before obtaining the warrants [in February]; the Cambridge Police Department did.” Government counsel did, indeed, have this chronology slightly wrong. The equipment was held in evidence by the MIT Police (rather than Cambridge Police) from its recovery on January 6th until February 3rd, when it was picked up and transported by SA Pickett and Det. Joseph Murphy to the Cambridge Police (Ex. A); the laptop and hard drive were fingerprinted by the Cambridge Police on February 10th (Ex. B); and the Secret Service executed warrants on the Cambridge Police Department taking custody of the evidence on February 25th.

Second, whether the Secret Service could have taken custody of the equipment on the date of Agent Pickett’s e-mail or even the day before when the evidence was recovered has never

been in issue. Of course the Secret Service could have. They obtained custody with the warrants and the warrants may not even have been necessary for the transfer of custody. The point is simply that the equipment was seized and held initially as evidence in a state case in which the Defendant had been charged with breaking and entering on MIT Property with intent to commit a felony. Federal law enforcement could, and did, rely in good faith on the fact that the equipment was being lawfully held as evidence in that state case while their own investigation proceeded.

Finally, and most importantly, there are four reasons, not one, that the interval between seizure of the equipment and obtaining a warrant was wholly proper. The e-mail is relevant only to a tertiary reason. The interval was wholly proper because:

- (1) Swartz's possessory interest in the equipment terminated when the equipment was properly seized as *physical* evidence that linked Swartz to his illegal downloads even without a search of its electronic contents. Just as a robbery defendant loses possessory interests in distinctive clothing left at the scene of the crime, so does a computer hacking defendant lose possessory interests in computer equipment left at the scene of the crime and taken from him incident to his arrest. Business records showed the laptop to have been purchased by Swartz and his thumbprint was found on the hard drive, justifying their seizure and retention pending trial even without an electronic search. (The e-mail is irrelevant on this point.)
- (2) Swartz's possessory interest in the equipment was highly attenuated even before the equipment's seizure — he left the laptop and attached hard drives unattended on MIT property for days on end while committing his thefts remotely. And, after he was caught, Swartz never sought return of the equipment or even copies of its contents until after he was charged in state and federal proceedings. (The e-mail is irrelevant on this point.)
- (3) Secret Service had no obligation to take custody of the equipment at any particular time from the Cambridge Police Department, which was holding it as evidence in Middlesex County's subsequently-indicted state case. (The e-mail is relevant to the Secret Service's uncontested opportunity to obtain custody when appropriate.)

- (4) The interval was not unreasonable in light of the facts of the investigation.  
(The e-mail is irrelevant on this point as well.)

The e-mail was not disclosed to Swartz late. The Government had first produced reports and e-mails relevant to the seizure of evidence and his arrest half a year before his suppression motions were due, and in both paper and electronic formats. Although this went well beyond the Government's obligations under *Brady* and the Local Rules, the Government wanted Swartz to readily explore grounds for arguing suppression and argue them fully, as he unquestionably did.

After preparing the Government's briefs and reading Swartz's reply, the Government reviewed the materials that had not been produced earlier again to ensure that they did not contain anything newly relevant and to continue the Government's practice of early disclosure. Two days after the Government saw the e-mail during its second thorough review of potential discovery materials, the Government hand-delivered it to Swartz's counsel in order to ensure counsel would have it well before the merits of his motion were argued or considered.

Respectfully submitted,

Carmen M. Ortiz  
United States Attorney

By: /s/ Stephen P. Heymann  
STEPHEN P. HEYMANN  
SCOTT L. GARLAND  
Assistant U.S. Attorneys

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/s/ Stephen P. Heymannnn  
STEPHEN P. HEYMANN  
Assistant United States Attorney

Date: January 9, 2013

**From:** Murphy, Joseph <jmurphy@cambridgepolice.org>  
**Sent:** Wednesday, February 23, 2011 4:52 PM (GMT)  
**To:** Heymann, Stephen (USAMA) <Stephen.Heymann@usdoj.gov>  
**Cc:** michael.pickett@usss.dhs.gov  
**Subject:** Evidence Movement

---

Please consider this email as written chronology for four pieces of evidence seized on January 6, 2011. These four items are

1 Acer Netbook/Laptop

1 Hard Drive Enclosure with cords

1 Hard Disk Drive – Western Digital

1 USB Thumb/Flash Drive

These items were grouped into two lots as they were recovered from two locations, the Netbook, HDD enclosure and HDD is one group and the USB Thumb/Drive being the other group.

The Cambridge Police headquarters has two secure areas with limited access on the third floor. One area being called the Property / Evidence Unit and the other being the Identification Unit Laboratory. The wall between these units has an installed evidence locker designed as a pass through system from Evidence to Identification for processing. Upon completion of analysis the items are passed back through the locker system from the Identification Unit back to Evidence.

February 3, 2011 at approximately 11:00am Special Agent Pickett and I (Joseph Murphy) received the four evidence items from MIT Police Sergeant Craig Martin.

We drove directly from MIT PD to Cambridge Police HQ

February 3, 2011 @ 11:27am the USB Thumb / Flash Drive was logged into Evidence and placed in the evidence locker.

February 3, 2011 @ 11:31am the Netbook, enclosure and HDD were logged into evidence and placed in the evidence locker.

February 3, 2011 @ 11:35am the USB Thumb / Flash Drive was taken from the locker and placed in the ID unit lab.

February 3, 2011 @ 11:35am the Netbook, enclosure and HDD were taken from the locker and placed in the ID unit lab.

February 11, 2011 @ 3:50pm the USB Thumb / Flash Drive was taken from the ID unit lab and placed in the locker.

February 11, 2011 @ 3:09pm the Netbook, enclosure and HDD were taken from the ID unit lab and placed in the locker.



Since February 11, 2011 the above mentioned items have been in the custody of the Evidence / Property Unit and been secured.

Will this timeline suffice? I have printed out the Custody information reports from CPD's database and will add those forms to the records being kept.

Joe

# EVIDENCE Processing Worksheet

Case #: 11-00078 Type of Crime: Computer CrimeDate Processed: [M T W (TH) F S Sun] 2/3/11 Time Processed: 11:35Processing Location: ☒ 125 Sixth St. (Station)☐ Other: \_\_\_\_\_Technician: Dolan / KardashianDate of Evidence Submission: 2/3/11Submitting Officer: Property

Suspect(s):

Aaron SWARTZ

Victim(s):

Officers Assisting:

NONE

Det. Assigned:

Murphy, JoePhotos Taken: ☒ Y ☐ N#of Photos: 7Total # of Packages Submitted: 2

INV #	Quantity	Evidence Description	Package Type	Results
EI (1)	(1)	Dash drive, black plastic, hp, 8GB, on silver metal tip, #0048WKRZ, label #15 #85102, below that is "V125W" price \$5.3x1.7x.08cm	(5) clear plastic 1RD evidence bag	
CS1 (1)	(1)	Mini laptop, black base w/ silver top reading "acer", make-acer, model: aspire one, S/N: LC8AX050010011001E1601, SNID: 00100550610, Model #NAV50, USB cord, 8 power cords (all black) connected to laptop, battery pack S/N: A20-10004 029800, for charging #6 se crime scene notes USB cord connects CSI + CS2, 25.9x18.3x2.5cm	(5) clear plastic evidence bag	4/6 + 2 add'l on 2/10/11
CS2 1	1	External Hard Drive Compartment silver w/ top bottom that separate from each other, top reads "rocketfish", bottom reads "RF 3.5" SATA HD Enclosure Kit RF-AH035", inside bottom is green electronic base w/ white labels w/ #s 8G056 9074 and 8K05: silver battery in this area has #8273 2A1, black USB cord connects bottom to CS1, 20.2x13.1x4.3cm	(5) clear plastic evidence bag	Neg
CS2a 1	1	External Hard Drive - Removable Unit black plus bottom w/ reflective silver metal top, on top is green + white label w/ product info: Western Digital, S/N: WMATA16210675, MDL: WD20EARS-00MVWB0, 2.0TB on bottom is green electronic panel w/ white label w/ # 2001-771698-102 AA, measures 10.3x14.5x2.4cm	(5) clear plastic evidence bag	Pos. 1LPL

-Det. Murphy came in @ 11:30 on 2/3/11 + took pictures of these items to use for the affidavit, packages were sealed then opened in ID Unit

MIME-Version:1.0  
From:ECFnotice@mad.uscourts.gov  
To:CourtCopy@localhost.localdomain  
Message-Id:4720993@mad.uscourts.gov  
Subject:Activity in Case 1:11-cr-10260-NMG USA v. Swartz Order on Motion for Leave to File  
Content-Type: text/html

**United States District Court**

**District of Massachusetts**

**Notice of Electronic Filing**

The following transaction was entered on 1/11/2013 at 12:03 PM EST and filed on 1/11/2013

**Case Name:** USA v. Swartz

**Case Number:** 1:11-cr-10260-NMG

**Filer:**

**Document Number:** 102(No document attached)

**Docket Text:**

**Judge Nathaniel M. Gorton: ELECTRONIC ORDER entered granting [100] Motion for Leave to File as to Aaron Swartz (1); granting [101] Motion for Leave to File as to Aaron Swartz (1); Counsel using the Electronic Case Filing System should now file the document for which leave to file has been granted in accordance with the CM/ECF Administrative Procedures. Counsel must include – Leave to file granted on (date of order)– in the caption of the document (Patch, Christine)**

**1:11-cr-10260-NMG-1 Notice has been electronically mailed to:**

Stephen P. Heymann Stephen.Heymann@usdoj.gov, Jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Michael J. Pineault mpineault@clementspineault.com

Scott Garland scott.garland@usdoj.gov, jodi.gird@usdoj.gov, usama.ecf@usdoj.gov

Matthias A. Kamber mkamber@kvn.com, plemos@kvn.com

Elliot R. Peters epeters@kvn.com, apicar@kvn.com, efiling@kvn.com, kbringola@kvn.com, klovet@kvn.com

Daniel E. Purcell dpurcell@kvn.com, jwinars@kvn.com

**1:11-cr-10260-NMG-1 Notice will not be electronically mailed to:**

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS**

UNITED STATES OF AMERICA,

v.

AARON SWARTZ,

Defendant.

No. 11-CR-10260-NMG

**Leave to File Granted by Electronic Order  
Dated January 11, 2013**

**DEFENDANT AARON SWARTZ’S SUPPLEMENTAL MEMORANDUM IN SUPPORT  
OF MOTIONS TO SUPPRESS**

Aaron Swartz requests the Court’s permission to supplement his Motions to Suppress and Dismiss (Dkts. 59-63) with a critical document only recently produced to Swartz by the Government. *See* Ex. A. The Government produced this document to Swartz for the first time in a letter dated December 14, 2012—after both the December 3, 2012, filing deadline for Swartz’s reply brief and the December 14, 2012 hearing where this Court considered whether to hold, and ordered, an evidentiary hearing on Swartz’s motions to suppress evidence.

The document at issue is an email from Secret Service Agent Michael Pickett to AUSA Stephen Heymann on January 7, 2011, *one day* after the Cambridge Police’s January 6, 2011 seizure of an ACER laptop, Western Digital hard drive, and HP USB drive from the MIT campus. Ex. A. In the email, Agent Pickett reports to AUSA Heymann that no one had yet sought a warrant to search the computer or flash drive, but that he was “prepared to take custody of the laptop anytime” after it was processed for prints by the Cambridge Police on the morning of January 7, “or whenever you [Heymann] feel is appropriate.” *Id.*

This email directly refutes the Government’s Opposition to Swartz’s pending motion to suppress evidence obtained from the laptop, hard drive, and USB drive. Dkt. 63. Swartz’s motion is based on the Government’s failure to obtain a search warrant for those items until February 9, 2011—*34 days* after the seizure and 33 days after the email exchange between Agent

Pickett and AUSA Heymann. In its Opposition, the Government argued that the 34-day delay was the fault of the Cambridge Police, not the Secret Service, and cannot be imputed to the federal Government. Specifically, the Government wrote:

The Secret Service did not seize [Swartz's] laptop, hard drive, or USB drive on January 6, 2011; the Cambridge Police Department did. ***Nor did the Secret Service possess this equipment before obtaining the warrants; the Cambridge Police Department did.*** Thus, the United States did not affect Swartz's possessory interest in his equipment until it executed warrants. ... Swartz cannot simply morph allegations that local police held evidence too long in a local prosecution into a claim that federal law enforcement officers did so in a subsequent federal case.

Dkt. 81 at 52-53 (emphasis added).

The newly-disclosed email shows that the Government's claim that it had no control over the seized equipment until on or shortly before February 9, 2011 is factually inaccurate. Agent Pickett's email makes clear that the Government had actual control over all the computer hardware at issue as of January 7, 2011—the day after the seizure—and could have taken physical custody of that hardware at any time. Moreover, the email shows that the lead prosecutor in this case not only was aware of this, but was personally directing the Secret Service regarding whether and when to take physical custody of the hardware.

Accordingly, this recently-produced email is not merely relevant to the pending motions to suppress, it directly refutes the Government's excuse for the 34-day delay. It shows that the Government not only had control over the hardware as of January 7, 2011, but was fully aware at that point of the hardware's evidentiary significance to this prosecution and its need to seek a search warrant. The Government could and should have sought and obtained a warrant promptly at that point. It certainly has no excuse for waiting over a full month to do so.

Finally, Swartz could not have submitted the email along with the pending motions or his reply papers, because—despite the email's relevance to the issues before the Court—the Government did not produce the email until December 14, 2012. Swartz has always diligently sought all available discovery in this case. Had the Government timely produced this email, Swartz would have submitted it to the Court at his earliest opportunity and also would have used

the email at the December 14, 2012 hearing. For all these reasons, Swartz requests that the Court consider the email in deciding Swartz's pending motions to suppress, so the Court may resolve the issues presented on a full factual record.

Dated: January 11, 2013

Respectfully submitted,

/s/ Elliot R. Peters

Elliot R. Peters (admitted *pro hac vice*)

Daniel Purcell (admitted *pro hac vice*)

Keker & Van Nest LLP

633 Battery Street

San Francisco, CA 94111

Tel.: (415) 391-5400

Fax: (415) 397-7188

Email: epeters@kvn.com

dpurcell@kvn.com

Michael J. Pineault

Clements & Pineault, LLP

24 Federal Street

Boston, MA 02110

Tel.: (857) 445-0135

Fax: (857) 366-5404

Email: mpineault@clementspineault.com

Attorneys for Defendant AARON SWARTZ

**CERTIFICATE OF SERVICE**

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing, and paper copies will be sent on January 11, 2013 to those indicated as non-registered participants.

Dated: January 11, 2013

/s/ Elliot R. Peters

Elliot R. Peters

# **EXHIBIT A**





**U.S. Department of Justice**

***Carmen M. Ortiz***  
*United States Attorney*  
*District of Massachusetts*

*Main Reception: (617) 748-3100*

*John Joseph Moakley United States Courthouse*  
*1 Courthouse Way*  
*Suite 9200*  
*Boston, Massachusetts 02210*

December 14, 2012

Elliot R. Peters  
Keker & Van Nest LLP  
633 Battery Street  
San Francisco, CA 94111-1809  
Via hand delivery

Re: U.S. v. Aaron Swartz

Dear Mr. Peters:

Enclosed you will find an e-mail which I came across while collecting supplemental discovery materials for you in the Swartz case. (The e-mail has been redacted, eliminating my communication to the agent and contact information. Mike Halsall, David Newman and Jay Perault, as with other MIT employees in this case, may be contacted through their counsel, Robert Ullman.) Because I thought you might find it useful in light of arguments in your recently filed reply brief, I am providing it to you early while I continue to go through the remainder of the materials.

Very truly yours,

CARMEN M. ORTIZ  
United States Attorney

By:

  
STEPHEN P. HEYMANN  
Assistant U.S. Attorney

**From:** MICHAEL PICKETT (BOS) <Michael.Pickett@uss.s.dhs.gov>  
**Sent:** Friday, January 7, 2011 3:25 PM (GMT)  
**To:** Heymann, Stephen (USAMA) <Stephen.Heymann@usdoj.gov>  
**Subject:** RE: Swartz Case

---

The laptop and external hard drive have been logged into evidence with MIT police. Cambridge Police will take the laptop and hard drive to process them for prints this morning. I am prepared to take custody of the laptop anytime after it has been processed for prints or whenever you feel is appropriate. As far as I know no one has sought a warrant for the examination of the computer, the cell phone that was on his person or the 8gb flash drive that was in his backpack. FYI the laptop and external hard drive were not on his person when he was arrested. They were traced by the laptop MAC address on the network, in a computer room in the MIT student center.

Mike Halsall has already provided me with a copy of the flow traffic. David Newman has made the packet capture available for download. I will download it today.

I will ask Mike Halsall for a copy of the surveillance.

Jay A Perault is the Captain from MIT Police that has been working with me during this investigation and was present during the arrest of Aaron Swartz.

Michael S. Pickett  
U.S. Secret Service  
Boston Field Office

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 11-10260-NMG
	)	
AARON SWARTZ,	)	Leave to File Granted 1-11-13
	)	
Defendant	)	

GOVERNMENT’S RESPONSE TO DEFENDANT’S SUPPLEMENTAL MEMORANDUM  
IN SUPPORT OF HIS MOTION TO SUPPRESS No. 5

The e-mail that Defendant Swartz’s supplemental memorandum cites as paramount to his fifth motion to suppress is relevant, but not nearly as important as he tries to make it out to be. In that January 7, 2011 e-mail, Secret Service Special Agent Pickett said that he was prepared to take custody of the equipment at issue — a laptop, an attached hard drive and a USB storage device — after it was processed for fingerprints or anytime thereafter.

First, Swartz claims that this contradicts the Government’s representation that “Nor did the Secret Service possess this equipment before obtaining the warrants [in February]; the Cambridge Police Department did.” Government counsel did, indeed, have this chronology slightly wrong. The equipment was held in evidence by the MIT Police (rather than Cambridge Police) from its recovery on January 6th until February 3rd, when it was picked up and transported by SA Pickett and Det. Joseph Murphy to the Cambridge Police (Ex. 1); the laptop and hard drive were fingerprinted by the Cambridge Police on February 10th (Ex. 2); and the Secret Service executed warrants on the Cambridge Police Department taking custody of the evidence on February 25th.

Second, whether the Secret Service could have taken custody of the equipment on the date of Agent Pickett’s e-mail or even the day before when the evidence was recovered has never

been in issue. Of course the Secret Service could have. They obtained custody with the warrants and the warrants may not even have been necessary for the transfer of custody. The point is simply that the equipment was seized and held initially as evidence in a state case in which the Defendant had been charged with breaking and entering on MIT Property with intent to commit a felony. Federal law enforcement could, and did, rely in good faith on the fact that the equipment was being lawfully held as evidence in that state case while their own investigation proceeded.

Finally, and most importantly, there are four reasons, not one, that the interval between seizure of the equipment and obtaining a warrant was wholly proper. The e-mail is relevant only to a tertiary reason. The interval was wholly proper because:

- (1) Swartz's possessory interest in the equipment terminated when the equipment was properly seized as *physical* evidence that linked Swartz to his illegal downloads even without a search of its electronic contents. Just as a robbery defendant loses possessory interests in distinctive clothing left at the scene of the crime, so does a computer hacking defendant lose possessory interests in computer equipment left at the scene of the crime and taken from him incident to his arrest. Business records showed the laptop to have been purchased by Swartz and his thumbprint was found on the hard drive, justifying their seizure and retention pending trial even without an electronic search. (The e-mail is irrelevant on this point.)
- (2) Swartz's possessory interest in the equipment was highly attenuated even before the equipment's seizure — he left the laptop and attached hard drives unattended on MIT property for days on end while committing his thefts remotely. And, after he was caught, Swartz never sought return of the equipment or even copies of its contents until after he was charged in state and federal proceedings. (The e-mail is irrelevant on this point.)
- (3) Secret Service had no obligation to take custody of the equipment at any particular time from the Cambridge Police Department, which was holding it as evidence in Middlesex County's subsequently-indicted state case. (The e-mail is relevant to the Secret Service's uncontested opportunity to obtain custody when appropriate.)

- (4) The interval was not unreasonable in light of the facts of the investigation.  
(The e-mail is irrelevant on this point as well.)

The e-mail was not disclosed to Swartz late. The Government had first produced reports and e-mails relevant to the seizure of evidence and his arrest half a year before his suppression motions were due, and in both paper and electronic formats. Although this went well beyond the Government's obligations under *Brady* and the Local Rules, the Government wanted Swartz to readily explore grounds for arguing suppression and argue them fully, as he unquestionably did.

After preparing the Government's briefs and reading Swartz's reply, the Government reviewed the materials that had not been produced earlier again to ensure that they did not contain anything newly relevant and to continue the Government's practice of early disclosure. Two days after the Government saw the e-mail during its second thorough review of potential discovery materials, the Government hand-delivered it to Swartz's counsel in order to ensure counsel would have it well before the merits of his motion were argued or considered.

Respectfully submitted,

Carmen M. Ortiz  
United States Attorney

By: /s/ Stephen P. Heymann  
STEPHEN P. HEYMANN  
SCOTT L. GARLAND  
Assistant U.S. Attorneys

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/s/ Stephen P. Heymannnn  
STEPHEN P. HEYMANN  
Assistant United States Attorney

Date: January 11, 2013

**From:** Murphy, Joseph <jmurphy@cambridgepolice.org>  
**Sent:** Wednesday, February 23, 2011 4:52 PM (GMT)  
**To:** Heymann, Stephen (USAMA) <Stephen.Heymann@usdoj.gov>  
**Cc:** michael.pickett@usss.dhs.gov  
**Subject:** Evidence Movement

---

Please consider this email as written chronology for four pieces of evidence seized on January 6, 2011. These four items are

1 Acer Netbook/Laptop

1 Hard Drive Enclosure with cords

1 Hard Disk Drive – Western Digital

1 USB Thumb/Flash Drive

These items were grouped into two lots as they were recovered from two locations, the Netbook, HDD enclosure and HDD is one group and the USB Thumb/Drive being the other group.

The Cambridge Police headquarters has two secure areas with limited access on the third floor. One area being called the Property / Evidence Unit and the other being the Identification Unit Laboratory. The wall between these units has an installed evidence locker designed as a pass through system from Evidence to Identification for processing. Upon completion of analysis the items are passed back through the locker system from the Identification Unit back to Evidence.

February 3, 2011 at approximately 11:00am Special Agent Pickett and I (Joseph Murphy) received the four evidence items from MIT Police Sergeant Craig Martin.

We drove directly from MIT PD to Cambridge Police HQ

February 3, 2011 @ 11:27am the USB Thumb / Flash Drive was logged into Evidence and placed in the evidence locker.

February 3, 2011 @ 11:31am the Netbook, enclosure and HDD were logged into evidence and placed in the evidence locker.

February 3, 2011 @ 11:35am the USB Thumb / Flash Drive was taken from the locker and placed in the ID unit lab.

February 3, 2011 @ 11:35am the Netbook, enclosure and HDD were taken from the locker and placed in the ID unit lab.

February 11, 2011 @ 3:50pm the USB Thumb / Flash Drive was taken from the ID unit lab and placed in the locker.

February 11, 2011 @ 3:09pm the Netbook, enclosure and HDD were taken from the ID unit lab and placed in the locker.

Since February 11, 2011 the above mentioned items have been in the custody of the Evidence / Property Unit and been secured.

Will this timeline suffice? I have printed out the Custody information reports from CPD's database and will add those forms to the records being kept.

Joe

# EVIDENCE Processing Worksheet

Case #: 11-00078 Type of Crime: Computer CrimeDate Processed: [M T W (TH) F S Sun] 2/3/11 Time Processed: 11:35Processing Location: ☒ 125 Sixth St. (Station)☐ Other: \_\_\_\_\_Technician: Dolan / KardashianDate of Evidence Submission: 2/3/11Submitting Officer: Property

Suspect(s):

Aaron SWARTZ

Victim(s):

Officers Assisting:

NONE

Det. Assigned:

Murphy, JoePhotos Taken: ☒ Y ☐ N#of Photos: 7Total # of Packages Submitted: 2

INV #	Quantity	Evidence Description	Package Type	Results
EI	(1)	Dash drive, black plastic, hp, 8GB, on silver metal tip, #0048WKRZ, label #15 #85102, label that is "V125W" price \$5.3x1.7x .08cm	(5) clear plastic 1RD evidence bag	
CS1	(1)	Mini laptop, black base w/ silver top reading "acer", make-acer, model: aspire one, S/N: LC8AX0B0010011001E1601, S/NID: 00100550610, Model #NAV50, USB cord, & power cords (all black) connected to laptop, battery pack S/N: A20-10004 029800, for charging #6 se crime scene notes, USB cord connects CSI + CS2, 25.9x18.3x2.5cm	(5) clear plastic evidence bag	4/6 + 2 add'l on 2/10/11
CS2	1	External Hard Drive Compartment, silver w/ top bottom that separate from each other, top reads "rocketfish", bottom reads "RF 3.5" SATA HD Enclosure Kit RF-AH035", inside bottom is green electronic base w/ white labels w/ #s 8G056 9074 and 8K05: silver battery in this area has #8273 2A1, black USB cord connects bottom to CS1, 20.2x13.1x4.3cm	(5) clear plastic evidence bag	Neg
CS2a	1	External Hard Drive - Removable Unit, black plus bottom w/ reflective silver metal top, on top is green + white label w/ product info: Western Digital, S/N: WMATA16210675, MDL: WD20EARS-00MVWB0, 2.0TB on bottom is green electronic panel w/ white label w/ # 2001-771698-102 AA, measures 10.3x14.5x2.4cm	(5) clear plastic evidence bag	Pos. 1LPL

-Det. Murphy came in @ 11:30 on 2/3/11 & took pictures of these items to use for the affidavit, packages were sealed then opened in ID Unit



UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA

v.

AARON SWARTZ

Criminal No. 11-10260-NMG


DISMISSAL

Pursuant to FRCP 48(a), the United States Attorney for the District of Massachusetts, Carmen M. Ortiz, hereby dismisses the case presently pending against Defendant Aaron Swartz. In support of this dismissal, the government states that Mr. Swartz died on January 11, 2013.

Respectfully submitted,

1/14/13  
Date

  
CARMEN M. ORTIZ  
United States Attorney

  
STEPHEN P. HEYMANN  
Assistant U.S. Attorney

Leave to File Granted:

Nathaniel M. Gorton, Judge  
United States District Court

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA

v.

AARON SWARTZ

)  
)  
)  
)  
)

Criminal No. 11-10260-NMG

DISMISSAL

Pursuant to FRCP 48(a), the United States Attorney for the District of Massachusetts, Carmen M. Ortiz, hereby dismisses the case presently pending against Defendant Aaron Swartz. In support of this dismissal, the government states that Mr. Swartz died on January 11, 2013.

Respectfully submitted,

1/14/13  
Date

Carmen M. Ortiz  
CARMEN M. ORTIZ  
United States Attorney

Stephen P. Heymann  
STEPHEN P. HEYMANN  
Assistant U.S. Attorney

Leave to File Granted:

N. M. Gorton 1/14/13  
Nathaniel M. Gorton, Judge  
United States District Court